


Privacy Policy

 English

This Privacy Policy describes Meazure Learning’s (“Meazure”) policies and procedures for the collection, receipt, use, storage, sharing, transfer, disclosure, and other processing of personal information through our websites, browser extensions, platforms, and applications, and any systems we control, including Scantron systems, (collectively, our “Services”), as well as your rights with respect to the information that we process about you. Meazure may obtain your information through your use of the Services or from your educational institution or certifying entity. When using any of our Services you understand that we will process your information consistent with the ways described in this Privacy Policy. We also may provide you with additional privacy disclosures and ask for your consent for the processing of certain information depending on the Services you are using. By accessing or using the Services, you agree to this Privacy Policy. This Privacy Policy may change from time to time (see Changes to this Policy below). Your continued use of the Services after we make changes is deemed to be acceptance of those changes, so please check the Privacy Policy periodically for updates. If you do not agree with the terms of this Privacy Policy, do not use our Services.

Information We Collect

Contacting Us: When you contact us through an online form, email, or through LiveChat, we will ask, if applicable, for information such as your name, email address, telephone number, job title/position, company name or educational institution, country/region of organization headquarters, current proctoring method, product you want to demo or services in which you are interested, information related to your exam situation, publication, certifying entity, and Meazure status (e.g., test taker, professor, or administrator) and information related to the exam type to be proctored. We may also ask you to provide us with information about the reason you are contacting us. We request this information so that we can accurately respond to your inquiries and address any support needs. We also collect any information you provide within your communications with us.

Downloading Whitepapers, Case Studies and eBooks and Signing Up for Our Newsletter: We may collect your email address and name.

Watching or Registering for Webinars: When you watch or register for one of our webinars, we may collect your name, email address, and company name.

Registering Accounts: When you create or reconfigure a Measure account or interact with our online portals, we may collect your name, username, password, candidate or user ID, date of birth, gender, language, email address, associated educational institution or certifying entity, contact phone number, fax number, department, title, challenge answer, notes, supervisor name and email address, information related to authored items (including discussions, dates, names, and times associated with the creation of and interaction with authored items or other events within the portals), information related to educational qualifications, information related to employers and previous experience, country of residence, time zone, any information you choose to upload, and for registrants in the United States, your residential address. You can also choose, but are not required, to provide us with additional phone numbers, your full residential address (non-U.S. users), and a profile picture using your device's camera (instructor registration only). We may also collect information related to your active exams and exam history and any accommodations you request. When you pay for an exam within your account, a third-party entity processes your payment. Measure may receive records of transactions, including purchase amount, name, and the last four digits of your credit card number. Records of your transactions with Measure are maintained within your account.

Please note that certain institutions and entities may configure their application instances to collect additional information. For example, certain institutions or entities may ask us to process medical documentation, marriage licenses, driver's licenses, and social security numbers on their behalf to determine testing eligibility and process candidate results. Our internal policies are designed to protect the confidentiality of personal information, restrict access, and prohibit their unlawful disclosure.

Testing: Before taking an exam, you must download our browser extension, using your username and password. Before your exam you must provide us with access to your device's camera and microphone and share your screen with our proctors through a LogMeIn File. We require you to share your photo ID on camera so that our proctors can verify your identity. Where your institution or organization requires it, we also use third-party biometric facial recognition software to augment our identity verification process. We also require you to perform a biometric keystroke measurement and answer identity verification questions for some exams if your institution or organization requires it. We use your biometric identifiers solely for identify verification and to ensure the security and integrity of the exams we proctor. Our identity verification providers delete biometric data immediately after each analysis. Measure does not sell, lease, trade, or otherwise profit from individuals' biometric data, and Measure does not permit its vendors or licensors to sell, lease, trade or otherwise profit from biometric data; provided, however, that Measure's vendors and licensors may be paid for products or services used by Measure that utilize such biometric data. If you would like a copy of our Biometric Information Policy, please contact us at the address in the *Contact Information* section below. During your exam, we continue to

monitor your screen, camera, and microphone in order to meet the requirements of your institution's testing parameters, communicate with you, and monitor your exam. Meazure may collect recordings of your test session for identity verification, exam integrity, and training purposes. We may also collect information related to test names, dates, results, proctors, status, and duration and other time-based metadata (including the amount of time spent answering each question), name, country, state/province, and city, proctor assessments, and certification number and status. If you opt in to the public display of your certifications, we will publicly display your certification number and status.

Applying for Jobs: When you apply to work for us through our website, we may collect your name, email address, phone number, cover letter, availability, website, blog, or portfolio, LinkedIn profile URL, references (including name, company, and contact info), city and state, resume, work eligibility status, information about whether you will now or in the future require sponsorship for employment visa status, information about prior employment with Meazure, information about whether you know anyone who works at Meazure (and, if yes, who), compensation range, information about your proximity to the office where you are applying, information about how you learned about the position, and information related to gender, ethnicity, disability, and veteran status. We request this information in order to satisfy our legal obligations and to evaluate your eligibility and qualifications for the open position.

Integrating with Learning Management Systems: When you access or use our Services, including for the purposes of registering for a Meazure-proctored test, through a learning management system integration, we may receive information about you, including information related to the exam, subject, date, registrants, and, if payment is required, payment information (though payment will be processed by our third-party payment processor).

Please note that while you are not required to provide us with your personal information, failure to provide us with certain categories of personal information may render you unable to use some or all of our Services.

Information Collected Automatically

Website Log Data: Our servers automatically record information ("Log Data") created by your use of the Services. Log Data may include information such as your IP address, browser type, the referring domain, internet service provider (ISP), operating system, date/time stamp, clickstream data, and browser plug-ins. We use this information to analyze trends, to administer our Services, to track users' movements around the Services and to gather demographic information about our user base as a whole.

Cookies: We use cookies or similar technologies to retain user settings, analyze trends, administer the Services, track users' movements around the Services, and to gather demographic information about our user base as a whole. Users can control the use of cookies at the individual browser

level. Our Services do not respond to “Do Not Track” signals except as set forth in the *Right to Opt Out* sections below. If you reject cookies, you may still use our Services, but your ability to use some features or areas of our Services may be limited. We also may use these technologies to collect information about your online activities over time and across third-party websites or other online services (behavioral tracking).

Interaction Data: We collect information about your interaction with certain components of our Services, including the resources that you access, pages viewed, how much time you spent on a page, and how you reached our Services. We also log the details of your visits to our Services and information generated in the course of using our Services, such as mouse movements, clicks, page visits, text entered, how long you spent on a page, and other details of your actions.

Third Parties and Tracking Technologies: Some content or applications on the Services are served by third parties. These third parties may use cookies alone or in conjunction with web beacons or other tracking technologies to collect information about you when you use our Services. The information they collect may be associated with your personal information or they may collect information, including personal information, about your online activities over time and across devices and different websites and other online services.

If you have any questions about targeted content, you should contact the responsible provider directly. For more information, see the *Third-Party Sharing* section below.

Testing: During testing, we automatically track your keystroke pattern to ensure it matches the biometric profile created before the start of your exam if your institution or organization requires it. We also obtain IP address information to help troubleshoot issues and verify your testing location.

How We Use Your Information

In addition to the uses described above, we may also use information that we collect about you or that you provide to us, including any personal information:

- To present our Services and their contents to you.
- To verify your identity.
- To present our Services and their contents to you.
- To provide you with information, products, or services that you request from us.
- To fulfill any other purpose for which you provide it.
- To improve and optimize our Services and their content and deliver better and more customized user experiences.
- To carry out our obligations and enforce our rights arising from any contracts entered into between you and us.

- To notify you about changes to our Services or any products or services we offer or provide through it.
- In any other way we may describe when you provide the information.
- For any other purpose with your consent.

Legal Bases for Processing

In most processing contexts, Measure acts as a processor or service provider for a controller educational institution or certifying entity. In those situations, we process personal data only on documented legally-compliant instructions from the controller entity. In the limited situations where Measure acts as a controller, we process your personal information, with your consent, where necessary to perform a contract, to comply with our legal obligations, and where doing so is in our legitimate interest and does not outweigh your rights and freedoms, such as to protect the integrity of our software, protect the integrity of our testing process, protect our intellectual property or the intellectual property of educational institutions or certifying entities, provide and improve our Services, and ensure compliance with applicable laws and our Terms of Service.

Third-Party Sharing

Analytics: Measure uses data analytics providers, including Google Analytics to help understand use of our Services. Google Analytics collects information sent by your browser as part of a web page request, including cookies and your IP address. Google also receives this information and their use of it is governed by their Privacy Policy. For more information about how Google Analytics collects and processes data, please visit [this link](#). To opt out of having your information used by Google Analytics, please visit [this link](#). For more information, please visit Google's privacy policy [here](#).

Advertising: Our third-party partners may use technologies such as cookies to gather information about your activities on our website and other websites in order to provide you advertising based upon your browsing activities and interests. If you wish to not have this information used for the purpose of serving you interest-based ads, you may opt out by [clicking here](#) (or if located in the European Union, [click here](#)). Please note this does not opt you out of all ads, only targeted ads. You will continue to receive generic advertisements online.

Additionally, third parties, including Google (through, for example, our use of Google Analytics Advertising Features on the measurelearning.com website, including Dynamic Remarketing), may place and read cookies on your browser, or use web beacons for the purposes of showing our ads on other websites or social media platforms. These third parties may use first-party cookies or other first-party identifiers and third-party cookies and other third-party identifiers for personalized and non-personalized advertising and measurement. Ad serving may be based on users' visits to our website or other websites on the Internet, and your activity may be tracked over time and across websites. We do not control these third parties' tracking technologies or how

they may be used. For information about how Google collects, shares, and uses data, please visit: <https://policies.google.com/technologies/partner-sites>. You can opt out of Google's use of cookies or device identifiers by visiting the Google Ads Settings web page at: <http://www.google.com/ads/preferences/>. For more information, please visit Google's privacy policy at: <https://policies.google.com/privacy?hl=en&fg=1>. You can opt out of a third-party vendor's use of cookies by visiting the Network Advertising Initiative opt-out page or control the use of device identifiers by using your device's settings.

Other Websites and Social Media: We share information with third-party apps and websites that integrate with our API or Services, or those with an API or Service with which we integrate. Our website includes links to other websites whose privacy practices may differ from those of Meazure. If you submit personal information to any of those websites, your information is governed by their respective privacy policies. We encourage you to carefully read the privacy policy of any website you visit. Our website also includes social media buttons and widgets for platforms such as Facebook, Twitter, YouTube (for more information about YouTube, see [Google's privacy policy](#), and LinkedIn. These features may collect your IP address, which page(s) you are visiting on our Services, and may set a cookie to enable the feature to function properly. Your interactions with these features are governed by the privacy policies of the companies providing them.

Your Institution: We may disclose information, including video and audio recording of your exam session, to your educational institution/certifying entity upon request. We do this so that your educational institution/certifying entity can verify that you were the person taking the exam and that no exam protocols were violated.

Service Providers: We may engage certain trusted third parties to help provide and optimize our Services and assist with our testing services, including assessment solutions providers, customer service support providers, human resources software providers, identification verification providers, learning management systems, payment processors, technology support services and technology providers, test administration sites, and webinar software platforms. We share your personal information with these third parties only to the extent necessary for them to perform the functions we have requested. These companies are authorized to use your personal information only as necessary to provide services to us in a manner consistent with our Privacy Policy and legal obligations.

Subsidiaries and Affiliates: We may disclose your personal information to our subsidiaries and affiliates.

Legal: In certain situations, Meazure Inc. may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. We may also disclose your personal information as required by law, such as to comply with a subpoena or other legal process, when we believe in good faith that disclosure is

necessary to protect our rights, protect your safety or the safety of others, investigate fraud, or respond to a government request.

Contracts: We may disclose your personal information to enforce or apply our Terms of Service, or our other agreements with you.

Business Transfers: Meazure may transfer information to a third party in the event of a bankruptcy, merger, acquisition, reorganization, or similar transaction. You will be notified via email and/or a prominent notice on our website of any change in ownership that affects the processing of your personal information, as well as any choices you may have regarding your personal information.

Other Sharing: We will also share your information when you provide us with consent to do so.

Data Retention

We retain information for as long as necessary to perform the Services described in this Policy, as long as necessary for us to perform any contract with you or your institution, or as long as needed to comply with our legal obligations.

Security

Once we no longer require information, we securely destroy it. We use commercially reasonable technical, organizational, and administrative measures to protect our Services against unauthorized or unlawful access or processing and against accidental loss, theft, disclosure, copying, modification, destruction, or damage. Nonetheless, we cannot guarantee that transmissions of your information will always be secure or that unauthorized third parties will never be able to defeat the security measures taken by us or our service providers. You play an important role in keeping your information secure. You should not share your user name, password, or other security information for your account with anyone. If you have reason to believe that your interaction with us is no longer secure (e.g., if you feel that the security of any account you might have with us has been compromised), please contact us immediately as detailed in the Contact Information section, below.

Any transmission of personal information is at your own risk. We are not responsible for circumvention of any privacy settings or security measures contained on the Services.

Children

Our Services are only provided to children with parental or guardian consent in accordance with applicable law. If you believe that a child has provided their information to Meazure without parental or guardian consent, please contact us as detailed in the Contact Information section, so that we can take steps to delete it.

Jurisdiction-Specific Rights

International Privacy Rights

To the extent required by applicable law, we provide you with the ability to access, correct, export, delete, withdraw consent, object to the processing of, or restrict processing of your personal information, to be informed of the existence, use, and disclosure of your personal information, and to confirm whether we hold any personal information about you. These functions will either be available within our Services, or you can contact us to submit a request. Note that if your request relates to information associated with your exam, you must submit your request through your testing institution or certifying entity as we are not the controller of that information. We will respond to your request in accordance with applicable regulations.

When the processing of your personal information is based on your consent, you have the right to withdraw or vary your consent at any time, but this will not affect any processing we have already performed.

We may need to obtain or confirm certain personal information in order to accommodate your request. We will not accommodate a request to change information if we believe the change would violate any law or legal requirement or cause the information to be incorrect.

In most processing contexts, Measure acts as a processor or service provider for a controller educational institution or certifying entity. In those situations, where required by applicable law, Measure only transfers personal data to third countries or international organizations where the controller educational institution or certifying entity has authorized Measure to do so and only where we have taken appropriate steps to ensure your privacy rights continue to be protected in accordance with applicable law.

Lodging Complaints: Pursuant to applicable law, you have the right to lodge a complaint with a supervisory authority in the EEA, the [Privacy Commissioner](#) in New Zealand, the [Privacy Commissioner](#) in Canada, the [Information Commissioner](#) in Australia, or the [Information Commissioner](#) in the UK if you believe we have processed your personal information in a manner inconsistent with your rights. We kindly request that you contact us first so that we may address your concern.

International Data Transfers: When you use the Services and provide information through the Services, Measure may transfer your information to a destination outside your jurisdiction, including to the United States. Measure, including its U.S. subsidiaries, relies on its certification under the Data Privacy Framework (“DPF”), the safeguards set forth in Article 46 of the GDPR, or derogations for specific situations set forth in Article 49 of the GDPR (or other analogous data transfer mechanisms) in order to transfer personal information across international borders. To request a copy of the specific Article 46 agreement(s) governing the transfer of your personal information, please email us at compliance@measurelearning.com.

In all cases, we will ensure that any transfers of personal information will only be undertaken in compliance with applicable data protection laws.

Information related to EU-U.S. Data Privacy Framework (“EU-U.S. DPF”), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (“Swiss-U.S. DPF”): Meazure (which includes all U.S. entities using the Meazure Learning brand name) complies with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF as set forth by the U.S. Department of Commerce. Meazure has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. DPF Principles with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Meazure has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. DPF Principles with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>.

DPF Internal Complaints Mechanism: In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, Meazure commits to resolve DPF Principles-related complaints about our collection and use of your personal information. EU, UK, and Swiss individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF should first contact Meazure at: compliance@meazurelearning.com.

DPF Recourse Mechanisms: In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, Meazure commits to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF to JAMS, an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit the JAMS website at: <https://www.jamsadr.com/DPF-Dispute-Resolution> for more information or to file a complaint. The services of JAMS dispute resolution are provided at no cost to you.

Please note that, under certain conditions, you may invoke binding arbitration to determine whether we have violated our obligations under the DPF Principles as to you and whether any such violation remains fully or partially unremedied. For more information regarding the possibility, under certain conditions, to invoke binding arbitration for complaints regarding DPF compliance that have not been resolved via other DPF mechanisms, please visit: <https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf>.

DPF Investigation & Enforcement: The Federal Trade Commission has jurisdiction over Meazure’s compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.

Liability in Cases of Onward Transfers to Third Parties: Measure has responsibility for the processing of personal data it receives under the DPF Principles and subsequently transfers to a third party acting as an agent on its behalf. Measure shall remain liable under the DPF Principles if its agent processes such personal data in a manner inconsistent with the DPF Principles, unless Measure proves that it is not responsible for the event giving rise to the damage.

U.S. State Privacy Rights

State consumer privacy laws may provide their residents with additional rights regarding our use of their personal information. To learn more about California residents' privacy rights, visit [here](#).

Colorado, Connecticut, Virginia, and Utah each provide their state residents with rights to:

- Confirm whether we process their personal information.
- Access and delete certain personal information.
- Data portability.
- Opt out of personal data processing for targeted advertising and sales.

Colorado, Connecticut, and Virginia also provide their state residents with rights to:

- Correct inaccuracies in their personal information, taking into account the information's nature and processing purpose.
- Opt out of profiling in furtherance of decisions that produce legal or similarly significant effects.

Connecticut and Utah also provide their state residents with rights to opt out of processing of sensitive personal data, including personal data that reveals an individual's citizenship or immigration status and the processing of biometric data.

-

To exercise any of these rights or appeal a decision regarding a rights request please see the *Exercising Your Rights* section in the CCPA policy below. Note that if your request relates to information associated with your exam, you must submit your request through your testing institution or certifying entity as we are not the controller of that information.

Nevada residents who wish to exercise their sale opt-out rights under Nevada Revised Statutes Chapter 603A may submit a request to this designated address: compliance@measurelearning.com. However, we do not currently conduct "sale" activities as defined under that statute.

Please note that where we collect or use personal information that does not individually identify you (also known as de-identified data), we will not attempt to re-identify such information.

CCPA Privacy Policy

California Residents

The following disclosures are made pursuant to the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (“CCPA”). These disclosures supplement any privacy notices we previously or contemporaneously provided to you, including any California-specific privacy notice provided to you if you are an employee of Meazure.

Right to Know

California residents have the right to be informed of the categories and specific pieces of personal information collected about them, including sensitive personal information, collected, used, and disclosed, the categories of sources from which that information is collected, whether that information is sold or shared, the categories of third parties to whom that information has been disclosed, the business or commercial purposes for collecting and using each category of personal information, and the intended retention period for each category of personal information.

The below reflects the categories of personal information we have collected from California residents during the past twelve months, the categories of sources from which the information was collected, the business or commercial purpose for which the information was collected, the categories of third parties to whom we disclosed that information, and our anticipated retention period for each category of information.

Test-Takers and Instructors

Personal Information Category set forth in Cal. Civ. Code § 1798.140

Personal identifiers, including real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license or passport number, or other similar identifiers.

California Customer Records personal information (Cal. Civ. Code § 1798.80(e)), including 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.

Characteristics of protected classifications under California or federal law.

Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

Internet and other electronic network activity information, including, but not limited to, browsing history, search history, and information about individual interactions with an Internet website, application, or advertisement.

Sensory data including audio, electronic, visual, thermal, olfactory, or similar information.

Professional or employment-related information

Non-public education information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 C.F.R. Part 99)

Source(s) of Personal Information Collection

Personal Identifiers: Directly from you; indirectly from you as you navigate or use our Services; internet service providers; your educational institution/certifying entity; devices you use to access our Services; learning management systems.

California Customer Records personal information: Directly from you; indirectly from you as you navigate or use our Services; internet service providers; your educational institution/certifying entity; devices you use to access our Services; learning management systems.

Characteristics of protected classifications: Directly from you; your educational institution/certifying entity; devices you use to access our Services.

Commercial information: Directly from you; indirectly from you as you navigate or use our Services; internet service providers; devices you use to access our Services; learning management systems.

Biometric information: You; Devices you use to access our Services.

Internet and other electronic network activity information: Indirectly from you as you navigate or use our Services; internet service providers; devices you use to access our Services; learning management systems.

Geolocation data: Indirectly from you; devices you use to access our Services

Sensory data: You; devices you use to access our Services.

Professional or employment-related information: You; your educational institution/certifying entity; devices you use to access our Services.

Non-public education information: Your educational institution/certifying entity; learning management systems.

Business or Commercial Purpose(s) for Collection/Use

Personal identifiers: Provide you with our Services; communicate with you; protect and secure our environment; verify, maintain, improve, upgrade, or enhance a product or service; identify and repair errors.

California Customer Records personal information: Provide you with our Services; communicate with you; protect and secure our environment; verify, maintain, improve, upgrade, or enhance a product or service; identify and repair errors.

Characteristics of protected classifications: Meet our legal obligations.

Commercial information: Process transactions; maintain transaction records; provide you with our products or services.

Biometric information: Provide you with our Services; protect and secure our environment; verify, maintain, improve, upgrade, or enhance a product or service; identify and repair errors.

Internet and other electronic network activity information: Detect security incidents; protect against malicious, deceptive, fraudulent, or illegal activity; verify, maintain, improve, upgrade, or enhance a service or device that is owned or controlled by us; identify and repair errors; perform analytics.

Geolocation data: Protect and secure our environment; verify, maintain, improve, upgrade, or enhance a product or service; identify and repair errors.

Sensory data: Provide you with our Services; communicate with you; protect and secure our environment; verify, maintain, improve, upgrade, or enhance a product or service; identify and repair errors.

Professional or employment-related information: Provide you with our Services; communicate with you; protect and secure our environment; verify, maintain, improve, upgrade, or enhance a product or service; identify and repair errors.

Non-public education information: Provide you with our Services; communicate with you; protect and secure our environment; verify, maintain, improve, upgrade, or enhance a product or

service; identify and repair errors.

Third Parties, Service Providers, and Contractors Receiving Personal Information Category

Personal identifiers: Affiliates; assessment solutions providers; certifying entities; customer service support providers; educational institutions; identity verification providers; live chat solutions; payment processors; technology providers and technology support services; test administration sites.

California Customer Records personal information: Affiliates; assessment solutions providers; certifying entities; customer service support providers; educational institutions; identity verification providers; live chat solutions; payment processors; technology providers and technology support services; test administration sites.

Characteristics of protected classifications: Affiliates; assessment solutions providers; certifying institutions; educational institutions; identity verification providers; technology providers and technology support services; test administration sites.

Commercial information: Affiliates; assessment solutions providers; certifying institutions; customer service support providers; educational institutions; payment processors; technology providers and technology support services; test administration sites.

Biometric information: Identity verification providers.

Internet and other electronic network activity information: Affiliates; assessment solutions providers; certifying institutions; customer service support providers; educational institutions; live chat solutions; payment processors; technology providers and technology support services; test administration sites.

Geolocation data: Affiliates; educational institutions; identity verification providers; technology providers and technology support services.

Sensory data: Affiliates; certifying institutions; customer service support providers; educational institutions; identity verification providers; live chat solutions; technology providers and technology support services.

Professional or employment-related information: Affiliates; certifying institutions; customer service support providers; educational institutions; identity verification providers; live chat solutions; technology providers and technology support services.

Non-public education information: Affiliates; assessment solutions providers; certifying institutions; customer service support providers; educational institutions; identity verification providers; live chat solutions; technology providers and technology support services; test administration sites.

Retention Period

Personal identifiers: The length of your business relationship with us plus any legally required additional retention period for this category of personal information following conclusion of your business relationship with us or two years post-relationship, whichever is longer.

California Customer Records personal information: The length of your business relationship with us plus any legally required additional retention period for this category of personal information following conclusion of your business relationship with us or two years post-relationship, whichever is longer.

Characteristics of protected classifications: The length of your business relationship with us plus any legally required additional retention period for this category of personal information following conclusion of your business relationship with us or two years post-relationship, whichever is longer.

Commercial information: The length of your business relationship with us plus any legally required additional retention period for this category of personal information following conclusion of your business relationship with us or two years post-relationship, whichever is longer.

Biometric information: Our identity verification providers delete biometric data immediately after each analysis.

Internet and other electronic network activity information: Barring any legally required additional retention period, up to one year.

Geolocation data: Barring any legally required additional retention period, up to one year.

Sensory data: The length of your business relationship with us plus any legally required additional retention period for this category of personal information following conclusion of your business relationship with us or one year post-recording, whichever is longer.

Professional or employment-related information: The length of your business relationship with us plus any legally required additional retention period for this category of personal information following conclusion of your business relationship with us or two years post-relationship, whichever is longer.

Non-public education information: The length of your business relationship with us plus any legally required additional retention period for this category of personal information following conclusion of your business relationship with us or two years post-relationship, whichever is longer.

Please note that we do not collect: precise geolocation (location within a geographical area of a circle with a radius of 1850 feet or less); racial or ethnic origin; religious or philosophical beliefs; union membership; genetic data; mail, email, or text messages where the content is not directed to us; personal information collected and analyzed concerning health; personal information collected and analyzed concerning sex life, or sexual orientation.

Website Visitors

Personal Information Category set forth in Cal. Civ. Code § 1798.140

Personal identifiers, including real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license or passport number, or other similar identifiers

California Customer Records personal information (Cal. Civ. Code § 1798.80(e)), including 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.

Characteristics of protected classifications under California or federal law.

Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

Internet and other electronic network activity information, including, but not limited to, browsing history, search history, and information about individual interactions with an Internet website, application, or advertisement.

Sensory data including audio, electronic, visual, thermal, olfactory, or similar information.

Professional or employment-related information.

Non-public education information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 C.F.R. Part 99)

Inferences drawn from any of the information identified above to create a profile about you reflecting your preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Source(s) of Personal Information Collection

Personal identifiers: Directly from you; indirectly from you as you navigate or use our Services; advertising networks; internet service providers; data analytics providers; devices you use to access our Services. For job applicants: recruiters; background check providers.

California Customer Records personal information: Directly from you. For job applicants: recruiters; background check providers.

Characteristics of protected classifications: Directly from you; indirectly from you as you navigate or use our Services; advertising networks; internet service providers; data analytics providers; devices you use to access our Services. For job applicants: recruiters, background check providers.

Commercial information: Directly from you; indirectly from you as you navigate or use our Services; advertising networks; internet service providers; data analytics providers; devices you use to access our Services.

Biometric information: We do not collect.

Internet and other electronic network activity information: Indirectly from you as you navigate or use our Services; advertising networks; internet service providers; data analytics providers; devices you use to access our Services; social networks.

Geolocation data: Indirectly from you; devices you use to access our Services; advertising networks; data analytics providers.

Sensory data: You; Devices you use to participate in our webinars or to call us.

Professional or employment-related information: For job applicants: directly from you; recruiters.

Non-public education information: For job applicants: directly from you; recruiters.

Inferences drawn from any of the information identified above to create a profile about you: Indirectly from you; devices you use to access our Services; advertising networks; data analytics providers

Business or Commercial Purpose(s) for Collection/Use

Personal identifiers: Provide you with our Services; communicate with you; protect and secure our environment; verify, maintain, improve, upgrade, or enhance a product or service; identify and repair errors; market to you.

For job applicants: Assess your application; satisfy legal obligations.

California Customer Records personal information: Provide you with our Services; communicate with you; protect and secure our environment; verify, maintain, improve, upgrade, or enhance a product or service; identify and repair errors; market to you.

For job applicants: Process your application; satisfy legal obligations.

Characteristics of protected classifications: Provide you with our Services; communicate with you; protect and secure our environment; verify, maintain, improve, upgrade, or enhance a product or service; identify and repair errors; market to you.

For job applicants: Process your application; satisfy legal obligations.

Commercial information: Maintain transaction records; provide you with our products or services; provide you with advertising or marketing services.

Biometric information: Not applicable.

Internet and other electronic network activity information: Detect security incidents; protect against malicious, deceptive, fraudulent, or illegal activity; verify, maintain, improve, upgrade, or enhance a service or device that is owned or controlled by us; identify and repair errors; provide you with advertising or marketing services; perform analytics.

Geolocation data: Protect and secure our environment; verify, maintain, improve, upgrade, or enhance a product or service; identify and repair errors.

Sensory data: Provide you with our Services; communicate with you; protect and secure our environment; verify, maintain, improve, upgrade, or enhance a product or service; identify and repair errors.

Professional or employment-related information: For job applicants: Process your application.

Non-public education information: For job applicants: Process your application.

Inferences drawn from any of the information identified above to create a profile about you:

Provide you with advertising or marketing services; perform analytics; maintain, improve, upgrade, or enhance a product or service.

Third Parties, Service Providers, and Contractors Receiving Personal Information Category

Personal identifiers: Advertising networks; affiliates; customer service support providers; data analytics providers; social networks; technology providers and technology support services; video hosting, sharing, and services platforms; webinar software platforms; background check providers and human resources software providers (for job applicants).

California Customer Records personal information: Technology service providers; customer relationship management providers; background check providers and human resources software providers (for job applicants).

Characteristics of protected classifications: Advertising networks; affiliates; customer service support providers; data analytics providers; social networks; technology providers and technology support services; video hosting, sharing, and services platforms; webinar software platforms; background check providers and human resources software providers (for job applicants).

Commercial information: Advertising networks; affiliates; customer service support providers; data analytics providers; social networks; technology providers and technology support services.

Biometric information: Not applicable.

Internet and other electronic network activity information: Advertising networks; affiliates; customer service support providers; data analytics providers; social networks; technology providers and technology support services; video hosting, sharing, and services platforms; webinar software platforms; human resources software providers (for job applicants).

Geolocation data: Advertising networks; affiliates; data analytics providers; social networks; technology providers and technology support services; video hosting, sharing, and services platforms.

Sensory data: Affiliates; customer service support providers; technology providers and technology support services; webinar software platforms.

Professional or employment-related information: Background check providers; human resources software providers; technology providers and technology support services (for job applicants).

Non-public education information: Background check providers; human resources software providers; technology providers and technology support services (for job applicants).

Inferences drawn from any of the information identified above to create a profile about you:

Advertising networks; affiliates; data analytics providers; social networks; technology providers and technology support services; video hosting, sharing, and services platforms.

Retention Period

Personal identifiers: The length of your business relationship with us plus any legally required additional retention period for this category of personal information following conclusion of your business relationship with us or three years post-relationship, whichever is longer.

California Customer Records personal information: The length of your business relationship with us plus any legally required additional retention period for this category of personal information following conclusion of your business relationship with us or three years post-relationship, whichever is longer.

Characteristics of protected classifications: The length of your business relationship with us plus any legally required additional retention period for this category of personal information following conclusion of your business relationship with us or three years post-relationship, whichever is longer.

Commercial information: The length of your business relationship with us plus any legally required additional retention period for this category of personal information following conclusion of your business relationship with us or three years post-relationship, whichever is longer.

Biometric information: Not applicable.

Internet and other electronic network activity information: Barring any legally required additional retention period, up to one year.

Geolocation data: Barring any legally required additional retention period, up to one year.

Sensory data: The length of your business relationship with us plus any legally required additional retention period for this category of personal information following conclusion of your business relationship with us or one year post-recording whichever is longer

Professional or employment-related information: Barring any legally required additional retention period, up to three years for non-hired applicants.

Non-public education information: Barring any legally required additional retention period, up to three years for non-hired applicants.

Inferences drawn from any of the information identified above to create a profile about you:

The length of your business relationship with us plus any legally required additional retention period for this category of personal information following conclusion of your business relationship with us or three years post-relationship, whichever is longer.

Sensitive Personal Information Category as set forth in Cal. Civ. Code § 1798.140

Social security number, driver's license number, state identification card, or passport number

Sources from which Information was Collected: For job applicants: recruiters; background check providers.

Purposes for Collection; Use: For job applicants: Process your application; satisfy legal obligations.

Third Parties, Service Providers, and Contractors Receiving Personal Information: Background check providers; human resources software providers; technology providers and technology support services (for job applicants).

Retention Period: Barring any legally required additional retention period, up to three years for non-hired applicants.

Please note that we do not collect: account access credentials (user names, account numbers, or card numbers combined with required access code, security code or password to access an account); precise geolocation (location within a geographical area of a circle with a radius of 1850 feet or less); racial or ethnic origin; religious or philosophical beliefs; union membership; genetic data; mail, email, or text messages where the content is not directed to us; unique identifying biometric information; personal information collected and analyzed concerning health; personal information collected and analyzed concerning sex life, or sexual orientation.

Right to Limit Use and Disclosure of Sensitive Personal Information

We do not collect or process sensitive personal information for the purpose of inferring characteristics about consumers. We also do not disclose sensitive personal information for purposes other than those specified in section 7027(m) of the CCPA regulations promulgated by the California Privacy Protection Agency. Therefore, we do not offer consumers the option to limit the use of their sensitive personal information.

Right to Opt Out of Sharing for Cross-Context Behavioral Advertising

In the past twelve months we have used data about your activities on our website to serve you ads on online properties owned or controlled by third parties. In the past twelve months, we have provided the following categories of information to advertising networks, affiliates, data analytics providers, social media networks, and video hosting, sharing, and services platforms for this purpose:

- Personal identifiers, such as unique personal identifier, online identifier, internet protocol address, device information and identifiers, and unique advertising identifiers and cookies; Internet and other electronic network activity information; geolocation information; characteristics of protected classifications under California or federal law; commercial data; and inference data.

If you would like to opt out of this sharing, you may exercise your right by modifying your cookie settings, or, you may do so in a frictionless manner by activating Global Privacy Control (“GPC”) opt out preference signal to opt out of disclosures of your personal information through the browser you are using. To learn more about how to activate the GPC, click [here](#).

Right to Opt Out of Sale

While we do not sell personal information in exchange for monetary consideration, we do share personal information for other benefits that could be deemed a “sale,” as defined by the CCPA. The CCPA broadly defines “sale” in a way that may include allowing third parties to receive certain information, such as cookies, IP address, and/or browsing behavior. In the past twelve months, we have provided the following categories of information to affiliates, data analytics providers, social media networks, and video hosting, sharing, and services platforms in ways that could be considered a “sale” under California law:

- Personal identifiers, such as unique personal identifier, online identifier, internet protocol address, device information and identifiers, and unique advertising identifiers and cookies; Internet and other electronic network activity information; geolocation information; characteristics of protected classifications under California or federal law; commercial data; and inference data.

We disclosed these categories of information to these third parties in order to market and advertise our products and services; perform analytics; and to maintain, improve, upgrade, or enhance our products or services.

We have no actual knowledge of selling the personal information or the sensitive personal information or minors under 16 years of age.

California residents have the right to opt out of the “sale” of their personal or sensitive personal information.

If you would like to opt out of such disclosures, you may exercise your right by modifying your cookie settings, or, you may do so in a frictionless manner by activating Global Privacy Control (“GPC”) opt out preference signal to opt out of disclosures of your personal information through the browser you are using. To learn more about how to activate the GPC, click [here](#).

Right to Delete Personal Information

You have the right to request the deletion of your personal information, subject to certain exceptions.

Right to Correct Inaccurate Personal Information

You have the right to request the correction of any inaccurate personal information that we maintain about you.

Right to Access

You have the right to request the categories and specific pieces of personal information we have collected about you.

Right of Non-Retaliation and Non-Discrimination

You have the right to exercise the privacy rights conferred to you under the CCPA without receiving retaliatory or discriminatory treatment. Company does not retaliate or discriminate against you for exercising the privacy rights conferred to you under the CCPA.

Exercising Your Rights

To exercise your rights, you may contact us via phone at 1-844-945-1453 or via email at compliance@measurelearning.com. Requesters will need to provide us with personal information in order to verify their identity and residency, including name, email, and state of residence. We will compare the information you provide with our internal records. The personal information that we use to verify identity and residency will not be used for any other purpose.

You may authorize an agent to submit a request on your behalf if you provide the authorized agent with written permission signed by you. Measure may require you to verify your identity directly with us and confirm that you provided the authorized agent with permission to submit a request on your behalf.

Changes to this Policy

We may update this Privacy Policy to reflect changes to our information practices. If we make any material changes, we will notify you by email (sent to the email address associated with your account) or by means of a notice on the Services prior to the change becoming effective. We encourage you to periodically review this page for the latest information on our privacy practices.

Contact Information

If you have questions about this Privacy Policy, or if you want to inquire about enforcing your individual privacy rights, please contact us using the information below:

Meazure Inc.

Attn: Compliance

7901 Jones Branch Dr, Ste 330

McLean, VA 22102

+1-844-945-1453

compliance@meazurelearning.com

Effective Date: January 1, 2023

Last Updated Date: May 6, 2024

