Proctortrack Privacy Policy

University of Toronto
August 23, 2024

Note: This Privacy Policy confirmed in our University of Toronto contract takes precedence over any other information published by Verificient Technologies.

Verificient Technologies Inc. ("Verificient", "Company" or "we" or "us" and/or "our") takes the privacy of all its stakeholders seriously. As such, we have set forth the following privacy policy:

Welcome to Verificient's Proctortrack Testing Platform ("Platform") which provides identity verification and test proctoring services. This privacy policy (the "Policy") outlines the policy adopted by Verificient, relative to the collection, use, storage, and disclosure of personal information on the site and on all related websites (together "Sites"), networks, applications, and other services provided by us, including the Platform (collectively, "Services"). Through this policy, we attempt to make information about how we handle personal information available.

Unless your sponsor institution or organization has arranged separate terms and provided you those terms in writing, or you have been provided different terms in writing by us, the terms of this policy apply to you and your relationship with us. Please take the time to familiarize yourself with this Policy and if you have any questions, please contact us at **privacy@verificient.com**. This policy is incorporated into and is subject to our Terms of Service.

Definitions*:*

Test Sponsor – Organization or academic institution that is requiring Identity Verification and high level of confidence that no breaches in the test integrity has occurred.

Data Controller – Organization or academic institution that requires collection of data of its users in order to ensure high integrity in their online credentials. The requirements needed for the test sponsor to deliver a high level of test integrity is dictated by the organization or institution. These high standards of identity verification is often outlined by federal guidelines and required for federally funded Title IV financial aid such as Federal Pell Grant, Federal Supplemental Educational Opportunity Grant (SEOG), Federal Perkins Loan, Federal Subsidized and Unsubsidized Direct Loans.

Data Processor – Verificient and its products (Proctortrack, Remotedesk) acts as a processor of data for the Test Sponsor and Data Controller. Processing includes ID

verification and ensuring that there has been no challenges to the test policy outlined by the Test Sponsor and Data Collector. Verificient temporarily stores the data in high-level encrypted data cloud storage facilities and destroys data (as per the outlined Data retention period) after submission.

Services We Provide

We provide Services on behalf of Test Sponsors who are our clients. They may be any institution, organization or unit of which you are a member (in any form, including but not limited to a user of their services) or an applicant or at which you are enrolled ("Test Sponsors"). Test Sponsors are organizations, educational institutions, or companies that offer and control any test that is used to make certification, licensure, or other types of decisions based on test results. We collect and/or receive personal information about a test taker in order to develop, administer, or proctor a test for a Test Sponsor. "Personal Information" is any information, such as name or email address, that identifies or can be used to identify the person to whom such information pertains, or is associated with a person. While providing Personal Information is voluntary, it is necessary if you are to obtain the grades, test scores, service, or credential that you seek from your Test Sponsor. We will handle and treat Personal Information collected or received while providing our Services in a manner that is consistent, first and foremost, with any binding agreement we have with your Test Sponsor. In the absence of a binding agreement, we will handle and treat your Personal Information in a manner that is consistent with this Policy and applicable law.

This Policy describes how we collect, use, store, and share information about you in connection with your use of the Services.

Information We Collect

Personal Information that you provide through the Services: We collect Personal Information (as per the requirements set by your Test Sponsor) after receiving consent from you, the user, such as when you:

- Launch the Services from your learning management system;
- Register for and/or login to the Platform; request customer support, a demo, or more information;
- Communicate with us via email or social media sites;
- Provide biometric data, including as part of onboarding to the Services, to create your identity profile; or take a test using our Services.

Personal Information collected through our Services may include the following:

- Name
- Photograph of identity document, such as a driver's license

- Photograph of you
- Telephone Number – (used for tech support only)
- Name of the Test Sponsor(s) (i.e., the educational institution(s)) at which you are enrolled and course test information
- E-mail address
- Test submissions
- Screen-captures
- Audio and video recordings of you taking tests
- Room scan- scan of the test-room environment
- Biometric data : Face and optionally, Knuckle voice scan, which may be considered as biometric information under certain regulatory regimes
- Hardware and software details (background process list, system configuration information, etc)
- Chat history between proctors or other customer support personnel and you.

Please be assured that the actual data collected is limited to the agreed categories (out of the above) with your Test Sponsor as per their proctoring requirements. You may check with your Test Sponsor's (your school or organization) Privacy Officer for details.

Information Provided By Test Sponsors: To enable our Services, your Test Sponsors may provide the following information,

- Name
- Email Address
- Government issued Identification number or associated details
- Learning Management System UserID

We may collect information about you from Test Sponsors, such as your email address, to provide you a registration link to our Services. This information may also be combined with the Personal Information collected from you.

Information which may be required but is not stored: Depending on the configuration of the Services by the Test Sponsor, you may be required to provide the following information, which is not stored on our System:

- Payment: **We do not collect and store Credit Card Information.** Certain Test Sponsors may require test takers to make proctoring payments themselves. "Stripe" is used as a third party payment gateway. Credit card information and address will be needed to complete the payment process **with Stripe** (only if you are required to make payments directly to us), **we do not collect or store credit card information**.
- Date of Birth (DOB): **We do not collect and store DOB records.** With certain Test Sponsors DOB may be required only for verification purposes during registration.

- Keystrokes: **We do not collect and store Keystroke Data.** We may only detect and restrict certain keystrokes to facilitate the test requirements.

Cookies and Other Tracking Technologies:

We use various technologies to collect information, including cookies. A cookie is a small file placed onto your device. Across the web, cookies do lots of different jobs, like letting you navigate between pages efficiently, storing your preferences, and generally improving your experience on a website. Cookies make the interaction between you and the website faster and easier. If a website does not use cookies, it will think you are a new visitor every time you move to a new page on the site – for example, when you enter your login details and move to another page it will not recognize you, and it will not be able to keep you logged in.

Our Services use cookies and similar technologies, such as web beacons, to identify your device and enable the functioning of our features, including the ability to log into your account, authentication, security, preferences retention, performance optimization, and data analytics.

If you do not want to receive cookies, you can change your browser settings. If you use our Services without changing your browser settings, we will assume that you've agreed to receive all cookies on the Company websites. Please note that our Services will not function properly without cookies.

Our Services may use two types of cookies, session and persistent. A session cookie expires after a set time, normally when you close your web browser. A persistent cookie remains after you close your web browser and may be used on subsequent visits to our Services to enable us to recognize you as an existing user.

We record certain information and store it in log files when you interact with our Services. This information may include IP address, browser information, device information, internet service provider, operating system, date/time stamp, and other system configuration information. We and our analytics providers also collect and store analytics information when you use our Services to help us improve our Services.

External Websites and Third Parties

From time to time, our Services may contain links to third party websites for example, Freshchat for providing support. The policies and procedures we describe in this Policy do not apply to the third party websites. The links from our Services do not imply that the Company endorses or has reviewed the third party websites. We suggest contacting those sites directly for information on their privacy policies before providing any of your personal information to them.

“Stripe” is used as a third party payment gateway. Stripe is only a channel used to accept payments and does not have access to any user data and no personal or user data is shared with Stripe **(except any data which you share directly with Stripe in making a payment)**. AWS (Amazon) and GCP (Google) are our cloud service providers. All the Data stored on the cloud servers is encrypted.

How We Use Your Personal Information

Verificient does not share or sell any information (including user data) to third parties.

We use your Personal Information generally as a data processor on behalf of the Test Sponsors, as per their requirement to provide, improve, and develop our Services. We do not use your Personal Information for any purpose other than delivering online integrity, as defined by your Test Sponsor. For instance, we use your Personal Information to register you for a test, answer any tech support questions or concerns you may have, administer the test, and/or convey the results of test integrity. We may also use your Personal Information to contact you about scheduling, technical, security, or other testing related issues, or to contact you for other administrative purposes, such as customer service. We use biometric data that we collect from you during onboarding to create your identity profile for the Services and for confirming your identity for when you take a test.

To Whom We Disclose Your Personal Information

When you take a test using the Services, we provide your Personal Information to the Test Sponsor(s) from whom you seek a test score, service, or credential to enable them to validate your identity and your test score, as well as for academic hearing purposes. For further information about how your Test Sponsor(s) may use your Personal Information, please contact your Test Sponsor(s).

We may also disclose your Personal Information in the following situations:

- When we believe it is reasonably necessary to comply with laws and regulations, or in response to a subpoena, court order, or other legal processes.
- To protect against misuse or unauthorized use of our Services, or to protect the security or integrity of our Services or any facilities or equipment used to make our Services available.
- To limit our legal liability and protect our property or other legal rights, or the rights of our Test Sponsors and test takers.
- To address actual or suspected fraud or other illegal activities.
- In the case of any merger, sale, acquisition, bankruptcy, liquidation, or other transfer of assets involving the company, any of your personal information which remains on the company’s servers at that time, may be transferred to and / or managed by the acquiring company or entity.

We may also seek your consent for additional disclosures of information, including your Personal Information, and will share it only as described to you.

Data Security

We take the security of your Personal Information seriously. We employ industry standard practices to protect your Personal Information in accordance with this Policy and applicable law. However, you should be aware that we do not control the security of your own equipment or your own network connection, and therefore any information you transmit to us through the equipment or internet connection you use, you transmit at your own risk.

Data Integrity

We take reasonable steps to ensure that the data we collect is reliable for its intended use. However, it is your responsibility to update us with any relevant changes in your personal information so that we can provide you with our Services. We collect Personal Information that is relevant for the purposes for which it is to be used. Furthermore, we take reasonable steps to ensure that we process Personal Information in a way that is consistent with the purposes for which it is collected.

Data Retention and Deletion

By default, data collected from proctored activities (including biometric data) are held for up to 180 days after a proctored test session and your identity profile and data collected for identification verification purposes (including the biometric data we use to create your identity profile) is retained for up to one year from the time the identity profile is created in our Platform.

However, your Test Sponsor has the capability to configure a custom data retention period as per their requirements, which shall always take precedence over our default data retention period.

After the applicable retention period, we will automatically purge (delete) your Personal Information from the Platform and our systems, and maintain only the minimal amount of data required for billing and necessary business purposes and legal compliance – which in most cases means the bare minimum, non-identifiable data, stored in an anonymised form to show certain session details such as the date, time, duration, and volume of sessions that took place. After the retention period, only your Test Sponsor has your data if they have exported from our system and retained it.

As explained above, we provide our Services as a processor on behalf of Test Sponsors who have the right to receive your data (e.g. for academic hearing purposes). We do not control what Test Sponsors do with your data. Test Sponsors have their own policies with respect to data retention and deletion. For further information on such policies, to revoke consent related to biometric data, or to request

deletion of any Personal Information outside of the retention policies described above, please contact the applicable Test Sponsor(s) (for example, your academic institution).

Please be aware: for any data deletion or data editing or data information or exercising any of your rights with regards to the data should be directed to the privacy office or officer of your Test Sponsor, academic institution or organisation, who is the Data Controller.

The Choices You Have With Your Information

Decisions regarding any request you make about your personal information data generally rest with your Test Sponsor (your Academic Institution or Organization) as the Data Controller, for whom Verificient is a Data Processor. If you created an account with us in connection with your use of the Services, you may modify or update some of your Personal Information by logging in and accessing your profile. You should be aware, however, that it is not always possible to completely remove or modify information in our databases. If you wish to access or modify any other Personal Information that we hold about you, you may contact us at **privacy@verificient.com**. If you have not created an account with us in connection with your use of the Services and wish to access or modify any Personal Information that we hold about you, please contact the applicable Test Sponsor(s), as they, by law, will generally have to approve any such request.

Verificient gives its users whose information we receive under the EU-U.S Data Privacy Framework (DPF), right to restrict the onward processing of their personal data and data portability, subject to certain limitations and exceptions as defined by your Test Sponsor. Any request related to change in use of the services, onward data processing or data portability should be directed to your Test Sponsor Privacy Officer. If for some reason, you are not able to contact your Test Sponsor then you may contact us at **privacy@verificient.com** or raise a ticket request at **https://www.verificient.com/support**.

International Users and International Data Transfer

In order to provide the Services, here is how we manage your Personal Information data:

Data collected for Test Sponsors located in Canada is stored within the Canada region. Data collected for Test Sponsors located in the EU is stored within the EU region. Other data by default is stored in the United States. Also, we may allow access to your data to other countries or regions in connection with the processing of data, fulfilling Test Sponsor's requests, and providing you the Services. We make such access available only to our own employees or authorised users (as defined by your Test Sponsors), as necessary to provide you the Services.

In the case of any such transfer or access, the personal information is subject to the law of the jurisdiction in which it is used or stored, including any law permitting or requiring

disclosure of the information to the government, government agencies, courts and law enforcement in that jurisdiction. By providing your information on or to the Services, you consent to any such storage, transfer, and processing in accordance with this Policy and applicable law.

Representation for Data Subjects in the EU and UK

We value your privacy and your rights as a data subject and have therefore appointed a EU & UK Privacy Representative as our point of contact.

Our EU & UK Privacy Representative provides you an easy way to exercise your privacy-related rights (e.g. requests to access or erase personal data). If you want to contact us via our representative or make use of your data subject rights, please visit : **EU & UK** privacy representative.

It may however be quicker to exercise your privacy rights by contacting the Data Privacy Officer of your sponsor institution.

Verificient Technologies Inc. adheres to the EU-U.S Data Privacy Framework (DPF) and Swiss-U.S. Data Privacy Framework Principles.

Note: Verificient adheres to EU General Data Protection Regulation (“GDPR“). Refer to our **GDPR page** for more information.

It may however be quicker to exercise your privacy rights by contacting the data privacy officer of your sponsor institution Verificient Technologies complies with the 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) as set forth by the U.S. Department of Commerce. Verificient Technologies has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (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. Verificient Technologies has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (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/**

Verificient Technologies Inc. is subject to the jurisdiction and enforcement authority of the US Federal Trade Commission (FTC).

In compliance with the EU-U.S Data Privacy Framework (DPF), Verificient Technologies Inc. commits to resolve complaints about our collection or use of your personal

information. EU, UK, and Swiss individuals with inquiries or complaints regarding our EU-U.S Data Privacy Framework (DPF) policy should first contact Verificient Technologies Inc. at: **privacy@verificient.com**, or contact our Support team at : **support@verificient.com**, or chat with us via the chat window on our website – **www.verificient.com**.

Verificient Technologies Inc. has further committed to refer unresolved privacy complaints under the Data Privacy Framework Principles to a U.S.-based independent dispute resolution mechanism, BBB NATIONAL PROGRAMS. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit **www.bbbprograms.org/dpf-complaints** for more information and to file a complaint. This service is provided free of charge to you.

If your EU-U.S Data Privacy Framework (DPF) complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See **https://www.dataprivacyframework.gov/s/article/G-Arbitration-Procedures-dpf?tabset-35584=2**

We acknowledge the right of EU, UK, and Swiss individuals to access their personal data. EU, UK, and Swiss individuals wishing to view or correct personal data may do so by following the instructions in this privacy policy found in “The Choice You Have With Your Information” section. Furthermore, said individuals also have the right to request deletion of data that has been handled in violation of the DPF Principles.

Verificient Technologies Inc. may be required to release the personal data of EU and Swiss individuals in response to lawful requests from public authorities including to meet national security and law enforcement requirements.

Verificient Technologies Inc. is liable for the onward transfer of personal data of EU and Swiss individuals to agent third parties unless it can be proven that we were not responsible for the actions giving rise to the damages.

You can view the complete Terms of Service **here**.

Your California privacy rights

This section provides additional details about the personal information we collect about California consumers and the rights afforded to them under the California Privacy Rights Act ‘CPRA’ which works as an addendum to the California Consumer Privacy Act or ‘CCPA’.

For more details about the personal information we have collected over the last 12 months, including the categories of sources of personal information collected, please see the “Information We Collect” section above. We collect this information for the business and commercial purposes described in the “How We Use Your Personal

Information" section above. We share this information with the categories of third parties described in the "To Whom We Disclose Your Personal Information" section above. Verificient does not sell the personal information we collect. Please note that we do use third-party cookies due to the technology of how Proctortrack is integrated with the testing platforms utilized by the Test-Sponsors and for continuous use of the App (Desktop app, mobile app or browser plugin/extension app) and for purposes as further described in our "Cookies and Other Tracking Technologies" section above.

Subject to certain limitations, the CPRA provides California consumers the right to request to know more details about the categories or specific pieces of personal information we collect (including how we use and disclose this information), the right to request deletion of their personal information, the right to opt out of any "sales" of their personal information that may be occurring and the right to not be discriminated against for exercising these rights.

California consumers may make a request pursuant to their rights under the CPRA by contacting your Test Sponsor Privacy Officer, or if for any reason you cannot contact your Test Sponsor Privacy Officer, toy may contact us at **privacy@verificient.com** Or may create a ticket request on **https://www.verificient.com/support**. We will verify your request using the information associated with your account along with the steps within our identifying process, including email address along with the assistance of your Test-Sponsor. Government identification may be required. Consumers can also designate an authorised agent to exercise these rights on their behalf.

Information from Children

Parental consent is required for use of the Services under the age of 13. We do not knowingly collect, maintain, or use personally identifiable information from children under the age of 13. We request that all visitors to our Sites who are under 13 years of age not disclose or provide any Personal Information. We encourage parents and legal guardians to monitor their children's Internet usage and to help enforce our Privacy Policy by instructing their children never to provide Personal Information on our Services without their permission. If we discover that a child under 13 years of age has provided us with Personal Information, we will take steps to delete such information.

Changes to this policy

Company reserves the right to change this Policy from time to time by posting an updated Policy to this site and the "last updated date" at the top of this page will be updated. We may also provide you additional notice, such as adding a statement to the home screen or sending you an email notification. Please review this Policy periodically, and especially before you provide any Personal Information. Your continued use of the Services after any changes or revisions to this Policy shall indicate your agreement with the terms of such revised Policy. The prior version of this policy can be found **here.**

Our Contact Information

Please contact us with any questions or comments you have about this Policy, your information, our use and disclosure practices, or our Services by email at **privacy@verificient.com**.