Last updated: August 18, 2023

OUR COMMITMENT TO PRIVACY

Vertical Screen, Inc., and its subsidiaries: Truescreen, Inc., Certiphi Screening, Inc. and Business Information Group, Inc. (collectively, "we," "us" or "Company"), are committed to safeguarding the privacy of the data we receive and process.

Sections

Applicability of Our Privacy Policy

This Privacy Policy describes our practices relating to your personal information in connection with the background screening, employment onboarding, and other services we provide to you and our clients. We are committed to collecting, storing, and using your personal information in compliance with all applicable laws, which may include the U.S. federal Fair Credit Reporting Act (“FCRA”) and other background screening and privacy laws.

By using our websites or other services, you consent to the collection and use of the information you provide according to this Privacy Policy.

Our websites are not directed at children under the age of 13.

Information We Collect

We collect personal information from you when you provide it or automatically when you engage with our websites or other products and services. We also collect personal information about you from our clients in connection with preparing a background screening report or providing other services to them. Examples of personal information we may collect from you or our clients include your name, address, date of birth, email address, national identification number (e.g. SSN), government-issued IDs and other identity verification documents, voice and video recordings, employment and education history, and other credentials related to your prospective employment or engagement for services.

We may also collect information from third parties in order to provide services to you and our clients, including: criminal justice agencies; law enforcement and other federal, state, and local agencies; federal, state, and local courts; the military; departments of motor vehicles and motor vehicle records

agencies; schools and learning institutions; licensing agencies; and credit bureaus and credit reporting agencies.

Examples of information we may collect from these third parties includes biographical data and information related to your employment and earnings history, residential history, education, credit history, motor vehicle history, criminal history and other public records, military service, identity verification, and professional credentials and licenses. Present and former employers and/or references may be contacted, and the report we prepare may include information obtained through personal interviews regarding your character, general reputation, personal characteristics and/or mode of living, in accordance with applicable law.

Our use and sharing of information we receive from a third party is covered by this Policy, but the third party's practices are covered by its own privacy notice. Although we make every effort to ensure that the data we collect and store about you is as accurate as possible, we cannot guarantee that third parties are accurate in information that is transmitted. We therefore are not responsible for the accuracy of data about you that may be supplied by any other third-party sources of information or our clients.

We use several forms on our websites and other methods to collect information about users. Examples of the types of information we collect when you access our websites may include, without limitation, the following:

1. Your name and the name of your company
2. Your electronic mail ("email") address
3. A contact address
4. Your phone and fax numbers
5. Any other information that you provide through our websites
6. The browser, operating system, and Internet Protocol address from which you accessed the website
7. Contents of any queries and search histories
8. What items you clicked on the applicable Web page

Some of the information we collect via our websites is gathered and maintained through the use of "cookies." A "cookie" is a small file that is saved on your computer where we maintain the "state" of your current visit to our website. We generally do not store any personal information in these cookies. Some of these cookies are created as "temporary" files that your browser should delete when the browser window is closed, while other cookies are stored for longer and indefinite periods of time ("persistent cookies").

Purposes for Collection

We provide background screening, identity and credential verification, application and onboarding, and related services to our clients. We use your personal information in order to provide and improve these services, to manage our contractual relationship with our clients, and to provide support to you and our clients in connection with these services.

We may also use information we collect to support our operations and customer satisfaction and quality management initiatives, to comply with our legal obligations, or as otherwise permitted or required by law. For example, if you dispute the accuracy of certain information and we update our reporting, we will retain and use information related to the dispute to help ensure our future reporting reflects that update.

Disclosure and Transfer of Your Information

We share your information with the individual(s) or business(s) that originally engaged us for the background screening or other services in accordance with applicable law. For example, we may share a background screening report and other information we collect from you and other parties with your prospective employer. Before we share information that is considered a "consumer report" for employment purposes under the FCRA, our clients are required to certify that they:

- Provided applicable disclosures to the subject that a background investigation will be performed and that personal data may be gathered for the purpose of completing the consumer report.
- Received authorization from the subject to obtain the consumer report; and
- Will not resell the consumer report to a third party.

We share information we collect with our personnel and may share it with our affiliates that are either subject to this Policy or follow practices at least as protective as those described in this Policy.

We may share some of your personal information with third parties who provide services to us or our clients, or assist us with providing services. For example, we may share some of your personal information with a third party that is assisting us with a specific background check or data validation, or with a website monitoring firm to monitor the use and traffic patterns of our websites. We may also share information with third parties when we use their tools and technologies to communicate with you (e.g. videoconferencing) or to assist with providing the services. These third-party service providers will have access to personal information needed to perform their functions, including to provide and improve their services, but may not use it for other purposes except as permitted or required by law.

We may share information with a third party that acquires all or part of our business, provided that such third party agrees to comply with the provisions of our Privacy Policy with respect to the use of the information unless you consent otherwise.

In certain instances, we may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, or may otherwise share certain information as permitted or required by law.

Lastly, we may share some of your personal information with other parties upon your request or authorization.

We will not rent or sell your personal information to other companies or individuals. Similarly, we do not compile mailing lists consisting of subjects of our screening reports for any purpose not related to a permissible use.

We may transfer your personal information to countries outside the country or region where you live or are employed/engaged, for example, when we or one of our service providers works with employees or technologies in other countries, in which case it may be subject to that specific country's laws.

Our Commitment to Data Security

We take reasonable procedures to protect personal information from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. We have physical, electronic, and managerial procedures in place to safeguard and secure the information we collect, including by limiting access to sensitive or personal information to authorized personnel. We encrypt data we process and securely store it in our self-hosted data centers in the United States or with our third party service providers who maintain similar levels of security.

It is also important that you to take adequate precautions to protect your personal information, including by using strong passwords, protecting against unauthorized access to your login credentials, and storing screening reports and other sensitive information in secure locations.

We keep your personal information for as long as we need it to fulfill the relevant purposes described in this Policy, or as permitted or may be required by law such as for tax or legal purposes, or as otherwise communicated to you. If we collect or receive any fingerprint data, we will securely store it on our servers within the United States and will retain it until the initial purpose for collecting the information or identifiers has been satisfied or for three (3) years from the individual's last interaction, whichever comes first, or longer if needed for purposes of fraud detection and investigation, pursuant to our legal obligations, or as otherwise communicated to you. Thereafter, we will promptly delete and permanently destroy the data.

Data Subject Rights

To the extent required by applicable law, you may have the right to access, correct, or delete your personal information. For example, the FCRA provides consumers with a right to access consumer reports and to dispute the accuracy of information contained in a consumer report, among other rights. You may also have a right to opt-out of any use or processing of your personal information collected by us. A request from a consumer to opt-out does not mean that the data is erased or deleted. However, while we may not be able to delete the information, we will process your opt-out in accordance with applicable law, for example by no longer allowing third parties to access the data.

If you wish to exercise any of your rights, please contact us at privacy@verticalscreen.com. We may request proof of identity before we disclose personal information to you, in accordance with our security procedures.

Data Privacy Framework (DPF)

Our Company commits to subject personal information we receive from the European Union, the United Kingdom (and Gibraltar), and/or Switzerland to the applicable DPF Principles.

Company 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. Company 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. Company 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 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/.

The certification is in the name of Vertical Screen, Inc. d/b/a Vertical Screen, Truescreen, Business Information Group and Certiphi Screening.

Recourse, Enforcement, and Liability

Company is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

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 Vertical Screen, Inc. at 1-800-260-1680 or Email: privacy@verticalscreen.com.

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Vertical Screen, Inc. 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 the International Centre for Dispute Resolution American Arbitration Association's (ICDR-AAA), 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 complaint to your satisfaction, please contact the American Arbitration Association by calling Jason Cabrera, International Liaison, at (212) 484- 3207 or Cabreraj@adr.org. You may also visit https://www.adr.org/search/adr for more information or to file a complaint. The services of American Arbitration Association are provided at no cost to you. **There is a possibility, under certain conditions, for you to invoke binding arbitration.**

Changes to our Privacy Policy

Our business and this Policy will change over time; you should regularly review this Policy to see recent changes and updates. If we update this Policy, we will update the "Last updated" date above

accordingly. Unless stated otherwise, our current Policy applies to all personal information that we have about you.

How to Contact Us

Should you have questions or concerns about this Privacy Policy or any other matter pertaining to our privacy practices, please write, call or send us an email to the following address:

Address:	Vertical Screen, Inc. Attn: Consumer Disclosure P.O. Box 541 Southampton, PA 18966
Phone:	1-800-260-1680
Fax:	1-888-495-8476
Email:	privacy@verticalscreen.com

For EU citizens subject to the General Data Protection Regulation (GDPR), Vertical Screen has appointed European Data Protection Office (EDPO) as its GDPR Representative in the EU. You can contact EDPO regarding matters pertaining to the GDPR:

- by using EDPO's online request form: https://edpo.com/gdpr-data-request/
- by writing to EDPO at **Avenue Huart Hamoir 71, 1030 Brussels, Belgium**

For UK citizens subject to the United Kingdom's General Data Protection Regulation (UK GDPR), Vertical Screen has appointed EDPO UK Ltd as its UK GDPR representative in the UK. You can contact EDPO UK regarding matters pertaining to the UK GDPR:

- by using EDPO's online request form: https://edpo.com/uk-gdpr-data-request/
- by writing to EDPO UK at **8 Northumberland Avenue, London WC2N 5BY, United Kingdom**