OUR COMMITMENT TO PRIVACY

Vertical Screen, Inc., and its affiliates: 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.

Effective as of April 28, 2023

Applicability of Our Privacy Policy

This Privacy Policy covers the information practices of Vertical Screen, Inc. and sets forth our privacy provisions relating to information submitted by our clients and their applicants and employees. This Policy also applies to other data that we collect from third parties and other sources in connection with our screening services. All data shall be collected, stored and used in compliance with applicable law, which may include the federal Fair Credit Reporting Act ("FCRA"); the European Union Data Protection Directive; and other national laws and state background screening and privacy laws.

By using our website, you consent to the collection and use of the information you provide according to this Privacy Policy. This Privacy Policy does not address any information or data we collect through traditional means (e.g., via telephone, fax or customer information forms, etc.).

Our website is not directed at children under the age of 13.

The Information We Collect and How We Use It

We provide employment screening services only to businesses with a permissible purpose in accordance with the FCRA. We release information via telephone, fax, mail and electronically, only to the individual(s) or business(s) that originally requested the service. We do not sell or provide the personal information collected and maintained in our databases to an outside entity for any purpose. Similarly, we do not compile mailing lists consisting of subjects of our screening reports for any purpose not related to a permissible use.

We use several forms on this website and other methods to collect personally identifiable information and other information about the users of this website ("you" or "user"). The types of information we collect when you access the website 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 in a form on the website
6. The Internet Protocol address from which you accessed the website

7. Contents of any queries
8. What items you clicked on the applicable Web page

In addition, we may collect other information not listed above. As appropriate, we may share any such data we collect with our affiliated companies or website monitoring firms strictly for monitoring and collecting information regarding the use and traffic patterns of our websites. However, the Company is required to and does comply with all applicable laws and regulations, some of which limit the collection, storage, use and dissemination of information.

We may also use any information we collect to support our customer satisfaction initiatives, and we may disclose any or all such information to 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.

Some of the information we collect via the website 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").

We may also collect certain non-personal data in connection with the website. For example, we may collect information on the browser that you use to access the website, such as keyword search history, the operating system that you are running, and certain information about the Web site you accessed immediately before you accessed our Web site.

We may aggregate your non-personal data with the non-personal data of our other users. We also collect and analyze general traffic patterns within our website to help maintain the flow and content of the website, and we may use some or all of this anonymous aggregated information to support our commercial activities, or for any other reason.

Personal information will be retained only as long as necessary to fulfill our consumer reporting services and/or client requirements, for a maximum period of seven (7) years, or as otherwise required by applicable laws. Information collected is securely stored in our self-hosted, fully-owned and controlled data centers, at our office locations within the United States. Fingerprint data is securely stored in our servers within the United States and will be permanently destroyed when the initial purpose for collecting the information or identifiers has been satisfied or after three (3) years from the individual's last interaction, whichever comes first.

Our Commitment to Data Security

To prevent unauthorized access to your personally identifiable information, maintain data accuracy and ensure the correct use of such information, we have put in place appropriate physical, electronic and

managerial procedures to safeguard and secure the information we collect. We urge you to take adequate precautions to protect your personal data.

Changes to our Privacy Policy

We reserve the right to revise this Privacy Policy from time to time in our discretion. If we modify this Privacy Policy, we will post the revised Privacy Policy, which will take effect immediately upon posting, and we may attempt to notify you of such change through your email address registered with us. It is your responsibility to periodically review this Privacy Policy.

Copyright

The copyright in all material provided on this site ("Site") is held by Company or by the original creator of the material. Except as stated herein, none of the material may be copied, reproduced, distributed, republished, downloaded, displayed, posted or transmitted in any form or by any means, including, but not limited to, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of Company or the copyright owner. You also may not, without Company's permission, "mirror" any material contained on this Site on any other server. Any unauthorized use of any material contained on this Site may violate copyright laws, trademark laws; the laws of privacy and publicity; and communications regulations and statutes.

Disclosure of Your Information

We will not rent or sell your Personal Information to other companies or individuals.

Transfers of Personal Data

For transfers of personal data from foreign countries, Company will ensure that it has an adequate transfer mechanism in place, such as the Standard Contractual Clauses or other country-specific clauses, where required by the country or territory holding the data. Any client contracting for services that would require international data transfers will be provided with our International Schedule for review and signature. Company further ensures that proper transfer mechanisms are in place with any sub-processor we contract with.

Our Company commits to cooperate with EU data protection authorities (DPAs) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) and comply with the advice given by such authorities with regard to human resources data transferred from the EU and Switzerland in the context of the employment relationship.

Onward Transfer

The information obtained by this Site is forwarded only to an entity that has been authorized by you to receive the data or an agent of our client (client is also known as the "End-user"), operating on behalf of the End-user. The information is only provided to the End-user for purpose described in the section under "Notice" below. Except as described in this Privacy Policy, or required by law, we will not use or

otherwise disclose any of the personally-identifying information that you provide or that we collect from third parties or other sources.

Company reserves the right to employ other companies and individuals as our subcontractors or vendors to perform functions on our behalf. All such contractors are contractually obligated to use and maintain the confidentiality of personal information in accordance with this Privacy Policy.

Company shall be liable in accordance with any applicable laws if found to have willfully violated consumer's rights in the onward transfer of personal data to third parties.

For personal data obtained from foreign countries, Company will have adequate transfer mechanisms in place, such as the Standard Contractual Clauses or other country-specific clauses, to allow for information from foreign countries to be provided to the End-user, via onward transfer, in a compliant manner.

Privacy Shield Provision of Privacy Policy

While the Privacy Shield has been invalidated with respect to data transfers to the United States, Company continues to comply with the Framework regarding all other data protection tenets such as the collection, use, and retention of personal information.

Company complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. Company has certified to the U.S. Department of Commerce that it, and the Policy, adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/

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

We comply with our obligations under the Privacy Shield Principles and the European Commission Directive on Data Protection, as follows:

Notice

Our background screening services include collection of information on individuals for employment-related purposes. Our clients provide us with your personal information in connection with our preparing a background screening report for them. Personal information gathered may include your history of employment and other credentials related to your prospective employment. In addition to the data that is submitted to us by our clients, we may collect data from third parties as needed to process academic, residential, achievement, job performance, attendance, litigation, personal history, credit reports, driving records, criminal history records and other lawful checks.

Prior employers and/or references may be contacted, and the report may include information obtained through personal interviews regarding the applicant's character, general reputation, personal characteristics and/or mode of living. We may provide all such information to our client (your current or prospective employer) in one or more reports. We will use such information only for the purposes of performing employment screening and credential verification services, including verification of the accuracy of the personal information and check of your references.

We are committed to subjecting all applicable personal data received from the EU to the General Data Protection Regulation "GDPR". In certain instances, we may be required to disclose personal information in response to lawful requests by public authorities, including meeting national security or law enforcement requirements.

Before the information we collect is provided to our clients, our clients must certify to us:

- That they will provide disclosure to their applicants that a background investigation will be performed and that personal data may be gathered for the purpose of completing the background screening report.
- That they will receive consent from an applicant before a Background Investigation Report is requested.
- That they will not resell the background report to a third party.

Choice (Opt-Out of Personal Information)

The information collected is only utilized for the purpose described above in the section on "Notice." In the event a consumer wishes to opt-out of any use of information collected by us, a consumer can notify us through the contact information on this website that permission or any use of the data is withdrawn. A request from a consumer to opt-out does not mean that the data is erased or deleted. Various laws require that this service maintain the data on file for a consumer for a period of time for the protection of the consumer as a result of applicable statute of limitations required under the federal Fair Credit Reporting Act. However, while we may not be able to delete the information, in the event of an opt-out, the data will no longer be made available to any third party or utilized by us for any purpose. The data will be securely stored on our systems for the remainder of the retention period.

Upon a receiving a request to delete fingerprint records specifically, we will purge the fingerprint record information.

If you are a U.S. resident and you do not wish to have your personal data made available to our client (your current or prospective employer), please do not authorize our client to procure a screening report from us.

If you are an E.U. resident, you may choose not to submit personal information to us through this website or through forms provided by our client for that purpose. By filling out and submitting the Authorization form, you expressly agree to provide personally-identifying information, and you

consent to our use of that information in accordance with our Privacy Policy. Notwithstanding the information stated above, we will approve any request from an E.U. resident for data to be deleted as required by the General Data Protection Regulation ("GDPR").

Security

We take all reasonable procedures to protect personal and identifiable information from loss, misuse and unauthorized access, disclosure, alteration and destruction. We have taken and will continue to take appropriate measures to assure the security of sensitive personal data. Encryption is used to secure the data we process. TLS version 1.2 encryption is used to ensure that data transmitted between our users and our websites is encrypted in transit. Password protection protocols are used on all computers. Access to servers containing private information and data is strictly limited to only our authorized personnel who have been trained to protect against loss, misuse, unauthorized access, disclosure, alteration or destruction of personal data under our control. We also do everything in our power to protect user information off-line. Users' information, not just the sensitive information mentioned above, is restricted in our offices. The servers that are used to store sensitive personal information are kept in a secure, state-of-the-art environment, with security measures.

Data Integrity and Purpose Limitation

Consistent with the Principles, personal information is limited to the information that is relevant for the purposes of processing. As previously mentioned, the information collected is only utilized for the purpose described above in the section on "Notice." Personal information is not processed in a way that is incompatible with the purpose for which it has been collected or subsequently authorized by the consumer. To the extent necessary and possible, reasonable steps are taken to ensure that data and information is reliable for its intended use, accurate, complete, and current.

Access

We provide you with access to applicable data collected about you in order to give you the reasonable opportunity to confirm what personal data we possess about you, and to correct, amend or delete information that is found to be inaccurate or incomplete. Disclosure is provided under the terms of the federal Fair Credit Reporting Act. You are entitled to a copy of your report under the terms of the FCRA. Company reserves the right to engage in reasonable efforts to confirm the identity of anyone requesting data, so that we only provide data to the consumer that is the subject of the data. For your protection, we will require proof of identity, including proper verification and confirmation that you are the individual who is entitled to request access, before providing information to you. If we collected information from you, we will mail to you, if you are a U.S. resident, a copy of the report about you within 5 days, as it has been provided to your current or prospective employer, at no charge.

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 and therefore, we are not responsible for the data. 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.

Recourse, Enforcement and Liability

This service verifies adherence to the Privacy Shield Policy by means of in-house verification by the management of this company. Company is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB).

In compliance with the Privacy Shield Principles and the GDPR, Company commits to resolve complaints about our collection or use of your personal information. EU and Swiss individuals with inquiries or complaints regarding our Privacy Shield policy should first contact Vertical Screen, Inc. at 1-800-260-1680 or Email: privacy@verticalscreen.com.

Company has further committed to refer unresolved Privacy Shield complaints to the International Centre for Dispute Resolution American Arbitration Association's (ICDR-AAA) Privacy Shield and Swiss-U.S. Dispute Resolution Program, an alternative dispute resolution provider located in the United States. If you do not receive timely acknowledgment of your 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://go.adr.org/privacyshield.html 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.**

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

Pursuant to Article 27 of 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 matters related to the 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