EU-US Privacy Shield / Swiss-US Privacy Shield

Introduction

Verify, Inc. and its subsidiaries Vendor Surveillance Corporation, VTR Inc., and Logistech (collectively "Verify" or "we") complies with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland. Verify, Inc. has certified that it adheres to the Privacy Shield Principles. If there is any conflict between the policies 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 page, please visit https://www.privacyshield.gov/

Scope

This Privacy Shield Policy applies to all Personally Identifiable Information (PII) collected by Verify subsidiaries; including Vendor Surveillance Corporation, VTR, Inc., Logistech, its contractors, customers, and other business partners located in the European Economic Area (the EEA) and Switzerland, which is then transferred to Verify in the United States. This includes, but is not limited to, transmission of data over phone lines, computer networks, and hard copy and includes such material as payroll or remittance records, telephone and contact records, business information, interviews and performance evaluations, contact details, results of permitted background and medical checks, resumes/CVs, bank accounts, and any material that identifies a particular individual employee, contractor, customer, or business partner in support of Verify service activities.

Responsibilities and Contact

In implementing this policy, Verify will annually certify to the US Department of Commerce that it agrees to adhere to the Privacy Shield principles. Verify further acknowledges that its failure to provide an annual self-certification to the US Department of Commerce will result in the removal of Verify from the list of participants.

Questions regarding the transmission of PII from the EEA or Switzerland to the United States or any other non-EEA country, or any further transmission of the PII once received in the United States, should be referred to Verify's Quality, Compliance and Administration department, at:

- Phone: +1-949-335-9120
- Mail: Verify – Quality, Compliance and Administration
  2525 Main St., Suite 100, Irvine, CA 92614, USA
- E-mail: compliance@vscnet.com

Policy

Verify's Privacy Policy is based on the principles of notice, choice, onward transfer, access, security, data integrity and enforcement with respect to PII and other sensitive data transferred out of the EEA or Switzerland to the United States or any other location.

- **Notice.** Verify will notify employees, contractors, customers and other business partners in the EEA/Switzerland about type(s) and purpose(s) for which personal data will be collected and used. Information will be provided on how individuals can contact Verify with inquiries or complaints regarding personal data. Verify will notify employees, contractors, customers, and other business partners of any third parties to which it discloses PII, and restrictions that limit the use and disclosure of such information.
- **Choice**. Prior to using PII for any purpose incompatible with the purpose for which it was originally collected or subsequently authorized or transferred to a third party exercising independent control over the data, Verify will give an individual employee, contractor, customer or business partner the opportunity to decline to have their data so used or transferred. In the event that the PII used for a new purpose or transferred to the control of a third party are sensitive personal data, the individual's explicit consent will be obtained prior to the use or transfer of the PII.
- **Onward Transfer**. Prior to transferring PII to any third party (excluding other members of the Verify group of companies), Verify will apply the Notice and Choice principles described above and will ensure that the third party recipient also subscribes to Privacy Shield Principles. Verify will further enter into a written agreement with such third party requiring that the third party provide at least the same level of PII protection as is maintained by Verify.
  In cases of onward transfer to third parties of data of EU or Swiss individuals received pursuant to the Privacy Shield, Verify, Inc. is potentially liable.
- **Access**. Verify acknowledges the individual's right to access their data to review, edit, correct, or delete it. Employees, contractors, customers and business partners covered under this Policy will have access to PII about them that Verify holds and will be able to correct, amend or delete information if it is inaccurate, excepting cases wherein the burden or expense of providing access would be disproportionate to the risks of the individual privacy in the case in question or the rights of persons other than the individual would be compromised or violated. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data, should direct their query to the contact information listed above.
- **Security**. Verify will take reasonable and appropriate administrative, technical and physical precautions to protect the confidentiality, integrity, and availability of PII, whether in electronic or tangible, hard copy form. Access to PII of EU/Swiss employees, contractors, customers and business partners will be limited to those users who require such access in the course of doing business.
- **Data Integrity.** Verify limits the collection, usage, and retention of information to that which is germane for the intended purposes for which it was collected, and takes reasonable steps to ensure that all PII is reliable, accurate, complete and current.
- **Enforcement**. To ensure compliance with these Privacy Shield principles, Verify will:
  - Commit to cooperate with the Data Protection Authorities (DPAs) of the EU/Switzerland in the investigation and resolution of complaints and will comply with any advice given by the DPAs;
  - Employ a procedure for verifying that the commitment the company has made to adhere to the Privacy Shield principles has been implemented;
  - Remedy issues arising out of any failure to comply with the principles;

- Conduct compliance audits of its relevant privacy and security practices to verify adherence to this Policy;
- Subject any employee determined to be in violation of this policy to disciplinary action, up to and including termination of employment

Dispute Resolution

The Verify Quality, Compliance and Administration department will be the internal organization and mechanism for ensuring compliance with the Privacy Shield principles and facilitating the internal compliance audits referenced above. Any questions or concerns regarding the use or disclosure of PII should be directed to the Quality, Compliance and Administration organization at the contact address, phone number, or website provided above. Verify will investigate and attempt to resolve complaints and disputes regarding use and disclosure of PII by reference to the principles contained in this Policy. For complaints that cannot be resolved between Verify and the complainant, Verify will participate in the following dispute resolution procedures:

- For disputes involving human resources/employment-related personal information received by Verify from individuals or citizens of EU countries or Switzerland, Verify has agreed to cooperate with the relevant Data Protection Authorities (DPAs) and to participate in the dispute resolution procedures of the panel established by the EU/Swiss DPAs.
- Verify, Inc. has further committed to refer unresolved consumer and non-human resources privacy complaints under the Privacy Shield Principles to BBB EU PRIVACY SHIELD, a non-profit alternative dispute resolution provider located in the United States and operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit www.bbb.org/EU-privacy-shield/for-eu-consumers/ for more information and to file a complaint.
- If your complaint is not satisfactorily addressed, and your inquiry or complaint involves human resource data transferred from Europe in the context of the employment relationship, you may have your complaint considered by an independent recourse mechanism: for EU/EEA Data Subjects, a panel established by the EU data protection authorities (“DPA Panel”), and for Swiss Data Subjects, the Swiss Federal Data Protection and Information Commissioner (“FDPIC”). To do so, you should contact the state or national data protection or labor authority in the jurisdiction where you work. CSC agrees to cooperate with the relevant national DPAs and to comply with the decisions of the DPA Panel and the FDPIC.
- Should your complaint remain fully or partially unresolved after a review by CSC, BBB EU Privacy Shield and the relevant DPA, you may be able to, under certain conditions, seek arbitration before the Privacy Shield Panel. For more information, please visit www.privacyshield.gov.
- Please note that if your complaint is not resolved through these channels, under limited circumstances, a binding arbitration option may be available to EU or Swiss individuals before a Privacy Shield Panel.
- Verify, Inc. is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

Limitation of Application of Principles

Verify adheres to these privacy principles except (a) as required or allowed by law; (b) to meet legal, governmental, law enforcement or national security obligations; or (c) to protect the health and safety of an individual.

NOTE: Verify, Inc. may be required to disclose an individual's personal information in response to a lawful request by public authorities, including to meet national security or law enforcement requirements.

Changes

This policy may be changed from time to time. When updates are made, the "Last Updated" date at the bottom of this document will be updated appropriately. This Policy will be posted on Verify's website and remain publically available at all times.

General Data Protection Regulation (GDPR)

Thank you for choosing to be part of our community at The Verify Group of Companies (Verify, Inc., Vendor Surveillance Corporation, VTR, Inc., VTR (UK) Staffing Ltd., Verify Europe Ltd., Verify Asia, Verify Canada, Inc.) ("Company", "we", "us", or "our"). We are committed to protecting your personal information and your right to privacy. If you have any questions or concerns about our policy, or our practices with regards to your personal information, please contact us at compliance@vscnet.com.

When you visit and use our website www.verifyglobal.com, you trust us with your personal information. We are committed to your privacy. In this privacy notice, we describe our privacy policy. We seek to explain to you in the clearest way possible what information we collect, how we use it and what rights you have in relation to it. We hope you take some time to read through it carefully, as it is important. If there are any terms in this privacy policy that you do not agree with, please discontinue use of our Sites and our services.

This privacy policy applies to all information collected through our website (such as www.verifyglobal.com), and/or any related services, sales, marketing or events (we refer to them collectively in this privacy policy as the "**Sites**").

Please read this privacy policy carefully as it will help you make informed decisions about sharing your personal information with us.

WHAT INFORMATION DO WE COLLECT?

Personal information you disclose to us

We collect personal information that you voluntarily provide to us when registering at the Sites expressing an interest in obtaining information about us or our products and services, when participating in activities on the Sites or otherwise contacting us.

The personal information that we collect depends on the contact of your interaction with us and the Sites, the choices you make and the product and features you use. The personal information we collect can include the following:

Name and Contact Data. We collect your first and last name, email address, postal address, phone number, and other similar contact data.

Credentials. We collect your passwords, password hints, and similar security information used for authentication and account access.

Payment Data. We collect data necessary to process payments, such as your payment instrument number (which may include credit card numbers and bank account numbers). All payment data is stored by our payment processor and you should review its privacy policies and contact the payment processor directly to respond to your questions.

All personal information that you provide to us must be true, complete and accurate, and you must notify us of any changes to such personal information.

Information automatically collected

We automatically collect certain information when you visit or navigate the Sites. This information does not reveal your specific identity (like your name or contact information) but may include device and usage information, such as your IP address, browser and device characteristics, operating system, language preferences, referring URLs, device name, country, location, information about how and when you user our Sites and other technical information. This information is primarily needed to maintain the security and operation of our Sites, and for our internal analytics and reporting purposes.

Like many businesses, we also collect information through cookies and similar technologies.

Information collected from other sources

We may obtain information about you from other sources, such as public databases, joint marketing partners, as well as from other third parties. Examples of the information we receive from other sources include: social media profile information; marketing leads and search results and links, including paid listings.

HOW DO WE USE YOUR INFORMATION?

We use personal information collected via our Sites for a variety of business purposes described below. We process your personal information for these purposes in reliance on our legitimate business interest ("Business Purpose"), in order to enter into or perform a contract with you ("Contractual"), with your consent ("Consent"), and/or for compliance with our legal obligations ("Legal relations"). We indicate processing grounds we rely on next to each purpose listed below.

We use the information we collect receive:

- To facilitate account creating and logon process with your Consent. If you chose to link your account with us to a third party *(such as your Google or Facebook account), we use the information you allowed us to collect from those third parties to facilitate account creation and logon process.

- To send you marketing and promotional communications for Business Purpose. We and/or our third party marketing partners may use the personal information you send to us for our marketing purposes, if this is in accordance with your marketing preferences. You can opt-out of our marketing email at any time (see the "**WHAT ARE YOUR PRIVACY RIGHTS"** below).

- To send administrative information to you for Business Purposes, legal Reasons and/or possible for Contractual. We may use your personal information to send you product, service and new feature information and/or information about changes to our terms, conditions and policies.

- Request feedback for our Business Purposes and/or with your consent. We may use your information to request feedback and to contact you about your use of our Sites.

- To protect our Sites for Business Purposes and/or for Legal Reasons. We may use your information as part of our efforts to keep our Sites safe and secure (for example, for fraud monitoring and prevention).

- To enforce our terms, conditions and policies for Business Purposes, Legal Reasons and/or possibly Contractual.

- To respond to legal requests and prevent harm for Legal Reasons. If we receive a subpoena or other legal request, we may need to inspect the data we hold to determine how to respond.

- For other Business Purposes. We may use your information for other Business Purposes, such as data analysis, identifying usage trends, determining the effectiveness of our promotional campaigns and to evaluate and improve our Sites, products, services, marketing and your experience.

WILL YOUR INFORMATION BE SHARED WITH ANYONE?

We only share and disclose your information in the following situations:

- **Compliance with Laws.** We may disclose your information where we are legally required to do so in order to comply with applicable law, governmental request, a judicial proceeding, court order, or legal process, such as in response to a court order or subpoena (including in response to public authorities to meet national security or law enforcement requirements).

- **Vital Interests and Legal Rights.** We may disclose your information where we believe it is necessary to investigate, prevent, or take action regarding potential violations of our policies, suspected fraud, situations involving potential threats to the safety of any person and illegal activities, or as evidence in litigation in which we are involved.

- **Vendors, Consultants and Other Third Party Service Providers.** We may share your data with third party vendors, service providers, contractors or agents who perform services for us or on our behalf and require access to such information to that work. Examples include: payment processing, data analysis, email delivery, hosting services, customer service and marketing efforts. We may allow selected third parties to use tracking technology on the Sites, which will enable them to collect data about how you interact with the Sites over time. This information may be used to, among other things, analyze and track data, determine the popularity of certain content and better understand online activity. Unless described in this Policy, we do not share, sell, rent or trade any of your information with third parties for their promotional purposes.

- **Affiliates.** We may share your information with our affiliates, in which case we will require those affiliates to honor this privacy policy. Affiliates include our parent company and subsidiaries, joint venture partners or other companies that we control or that are under common control with us.

- **Business Partners.** We may share your information with our business partners to offer you certain products, services or promotions.

- **With your Consent.** We may disclose your personal information for any other purpose with your consent.

- **Other Users.** When you share personal information or otherwise interact with public areas of the Sites, such personal information may be viewed by all users and may be publicly distributed outside the Sites in perpetuity. Similarly, other users will be able to view descriptions of your activity, communicate with you within our Sites, and view your profile.

DO WE USE COOKIES AND OTHER TRACKING TECHNOLOGIES?

We may use cookie and similar tracking technologies (like web beacons and pixels) to access or store information. Specific information about how we use such technologies and how you can refuse certain cookies is set out in our Cookie Policy.

DO WE USE GOOGLE MAPS?

This website, mobile application, or Facebook application uses Google Maps APIs. You may find the Google Maps APIs terms of service here. To better understand Google's privacy policy, please refer to this link.

By using our Maps API Implementation, you agree to be bound by Google's Terms of Service.

IS YOUR INFORMATION TRANSFERRED INTERNATIONALLY?

Our servers are located in United States. If you are accessing our Sites from outside United States, please be aware that your information may be transferred to, stored, and processes by us in our facilities and by those third parties with whom we may share your personal information.

If you are a resident in the European Economic Area, then these countries may not have data protection or other laws as comprehensive as those in your country. We will however take all necessary measures to protect your personal information in accordance with this privacy policy and applicable law.

HOW LONG DO WE KEEP YOUR INFORMATION?

We will only keep your personal information for as long as it is necessary for the purposes set out in this privacy policy, unless a longer retention period is required or permitted by law. No purpose in this policy will require us keeping your personal information longer than required per established regulations and contractual obligations.

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize it, or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

HOW DO WE KEEP YOUR INFORMATION SAFE?

We have implemented appropriate technical and organizational security measures designed to protect the security of any personal information we process. However, please also remember that we cannot guarantee that the internet itself is 100% secure. Although we will do our best to protect your personal information, transmission of personal information to and from our Sites is at your own risk. You should only access the services within a secure environment.

HOW DO WE COLLECT INFORMATION FROM MINORS?

We do not knowingly solicit data from our market to children under 18 years of age. By using the Sites, you represent that you are at least 18 or that you are the parent or guardian of such minor and consent to such minor dependents use of the Sites. If we learn that personal information from users less than 18 years of age has been collected we will deactivate the account and take reasonable measures to promptly delete such data from our records. If you become aware of any data we have collected from children under age 18, please, contact us at compliance@vscnet.com

WHAT ARE YOUR PRIVACY RIGHTS?

In some regions (like the European Economic Area), you have certain rights under applicable data protection laws. These may include the right (i) to request access and obtain a copy of your personal information, (ii) to request rectification or erasure; (iii) to restrict the processing of your personal information; and (iv) if applicable, to data portability. In certain circumstances, you may also have the right to object to the processing of your personal information. To make such a request, please use the contact details provided below. We will consider and act upon any request in accordance with the applicable data protection laws.

If we are relying on your consent to process your personal information, you have the right to withdraw your consent at any time. Please note however that this will not affect the lawfulness of the processing before its withdrawal.

If you are a resident in the European Economic area and you believe we are unlawfully processing your personal information, you also have the right to complain to your local data protection supervisory authority. You can find their contact details here: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

Account Information

If you would at any time like to review or change the information in your account or terminate your account, you can:

- Log into your account setting and update your user account
- Contact us using the contact information provided

Upon your request to terminate your account, we will deactivate or delete your account and information from our active database. However, some information may be retained in our files to prevent fraud, troubleshoot problems, assist with any investigations, enforce our terms of Use and/or comply with legal requirements.

Cookies and similar technologies: Most Web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove cookies and to reject cookies. If you choose to remove cookies or reject cookies, this could affect certain features or services of our Sites.

Opting out of email marketing: You can unsubscribe from our marketing email list at any time by clicking on the unsubscribe link in the emails that we send or by contacting us using the details provided below. You will then be removed from the marketing email list – however, we will still need to send you service-related emails that are necessary for the administration

- Access your account settings and update preferences.
- Contact us using the contact information provided.

DO WE MAKE UPDATES TO THIS POLICY?

We may update this privacy policy from time to time. The updated version will be indicated by an updated “Revised” date and the updated version will be effective as soon as it is accessible. If we make material changes to this privacy policy, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this privacy policy frequently to be informed of how we are protecting your information.

HOW CAN YOU CONTACT US ABOUT THIS POLICY?

If you have questions or comments about this policy, you may contact our Data Protection Officer (DPO), by email at compliance@vscnet.com, by phone at 949-335-9120, or by post to:

The Verify Group of Companies
2525 Main Street, Suite 100
Irvine, CA 92614
United States

If you are a resident in the European Economic Area, the "date controller" of your personal information is The Verify Group of Companies. We have appointed a local Data Protection Officer to be its representative in the EEA. You can contact them directly regarding the processing of your information by email at compliance@vscnet.com, or by post to:

The Verify Group of Companies
8 Clarendon Drive
Wymbush
Milton Keynes, Buckinghamshire MK8 8ED
United Kingdom