PRIVACY POLICY

Last updated: February 2024

Introduction

ARISCU (Green Gain Africa (Pty) Ltd, Registration No. 2013/125736/07 and Green Gain Consulting (Pty) Ltd, Registration No. 2002/019249/07) was acquired by Veriforce LLC, a leading Supply Chain Risk Performance Network, during 2018. Reference herein after to "Veriforce" shall therefore include ARISCU.

This Privacy Policy describes how and why Veriforce might collect, store, use and/or share your information when you use our services via our websites, applications and other platforms that are owned by Veriforce, or engage with us in other related ways, including any sales, marketing events, phone call or email.

This Privacy Policy covers all applicable jurisdictions where we do business and does not exclude any jurisdictions that are not specifically mentioned herein.

We may need to update this Privacy Policy from time to time. Where a change is significant, we'll make sure we let you know by sending you an email or by posting a visible notice on our Applications and websites.

If you have any questions or concerns, please contact us at privacy@veriforce.com or in South Africa at info@ariscu.com.

About US

Veriforce LLC https://veriforce.com/, and https://veriforceone.com ('we' or 'our' or 'us') is a US registered company with offices in Houston, TX and offices in Covington, LA and Calgary and Toronto, Canada, as well as in Pretoria, South Africa, Merton, UK and Australia. Our "Affiliate(s)" are companies that are under Veriforce common ownership.

We provide easy-to-use global online compliance, management and training platforms ("Applications") and associated services for businesses of all sizes that require end-to-end supply chain risk and compliance management solutions. If you want to find out more about what we do, see the What We Do - Veriforce page.

Our Applications and associated services may be contracted by:

- Legal entities, corporations, professional associations and sole proprietors for the purpose of hiring and managing their own supplier workforce ('Client');
- Legal entities, corporations, professional associations and sole proprietors who are in the business of providing various services to other entities as their suppliers ('Supplier');

- Client and Supplier are given access to a dedicated account. Further access rights and permissions to their accounts are granted to their employees and other third parties (“End Users"), as solely decided by them.
- Individuals (“End Users”) may also access our Services directly for their benefit.

Clients, Suppliers and End Users altogether referred to as ‘Customers’.

How the Compliance Applications Work

The Applications functionality allows:

- Suppliers to promote their business profile to Client within the Applications as required by the Clients or Recognised Assessment Bodies;
- Clients or Suppliers to maintain and/or manage Users personal profile within the Applications.

This Privacy Policy applies to personal information or personal data collected by us for the purpose of providing the Applications and contracted services. We collect and process all personal data under Clients’, Suppliers’ and ‘End Users’ strict guidance and instructions.

What information we collect and how

We collect information by fair and lawful means and limit the collection to the personal information that is necessary for us to provide services under an Order Form. We collect personal information that you voluntarily provide to us when you express an interest in obtaining information about us or our products and services, when you participate in activities on the services, or otherwise when you contact us, in particular:

We collect information directly from you when:

- When you sign up to receive our news, updates and marketing communications, we collect your name and email address and the name of the company you work for or represent. You may unsubscribe at any time from these communications by clicking the “Unsubscribe” link in the email.
- When you contact us via the Live Support feature in the Applications, we collect your name, email address, phone number and any personal information you may include in the chat with the support staff.
- When you call us directly with questions, inquiries and support issues, we collect your name, contact details (phone, email address, company you work for or represent) and any personal information you may include in the call. We may also record the call for training purposes.
- When you email us, we collect your name and email address as well as the information you include in the email.
- When you enter or upload any information about yourself in the Applications sites, for example your name, address, employer, your training courses, your qualifications.

- When you purchase an online course or service on our Applications, we collect your name, email address, transaction information and financial details. We also retain your purchase history.
- When you apply for a job with us, we may collect your name, phone number, email address, work history and your qualifications.

We may collect information about you from other parties, for example your employer, when information is manually entered or uploaded to the Applications sites. The personal information always collected is:

- first and last names, job position, contact details (business email, telephone number) and physical address
- records of assigned and completed training courses and orientations

Other information is also collected which may relate to the business that has contracted our services. If the business is a sole trader or an incorporated business, the information may be considered personal information:

- professional licenses, certifications, qualifications, insurance issued to individuals
- job hazard assessments, audits and inspections reports
- compliance evaluation results and scores
- incident information related to an individual
- worker compensation certificates (no medical details are recorded)
- notes entered by Clients, Suppliers or other authorized End Users

We collect personal information from Clients or Suppliers who require us to invite their existing suppliers/subcontractors to contract our services. You may be one of these subcontractors ('End Users'). The personal information received from Clients or Suppliers may include:

- End User business name
- name of End User's representative
- representative's contact details - address, phone number, email
- representative's job role
- social security number (truncated to last 4 digits))
- geolocation

When necessary, with your consent or as otherwise permitted by applicable law, we process the following categories of sensitive information:

- social security numbers or other government identifiers
- geolocation

We may collect data necessary to process your payment if you make a purchase, such as your payment instrument number and the security code associated with your payment instrument.

We may also obtain some of the above personal information about you from third parties (other individuals or organisations) or from publicly available sources, for example social networks, company websites and public records.

Clients, Suppliers and End Users are responsible to ensure the submission of any personal information to the Applications and to Veriforce, is compliant with all applicable privacy laws, regardless of jurisdiction. Clients, Suppliers and End Users are also responsible to ensure compliance with applicable privacy laws when deciding to share their account profiles with other Customers.

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

We collect Information automatically

We automatically collect certain information when you visit, use, or navigate through our services, including system log files. This information does not reveal your specific identity (like your name or contact information) but may include device and usage information, such as your Internet Protocol addresses, browser and device characteristics, internet service provider, operating system, language preferences, pages visited within our Applications, referring/exit pages, search terms, operating system, date/time stamp, and clickstream data, device name, country, location, information about how and when you use our services, and other technical information.

We collect and track information automatically ("System data") when you visit our Applications:

- http requests (requests sent by the Customer to trigger an action on the server)
- IP address of end users
- statistical and other information related to the performance, operation and use of the Applications and data related to identifiable End Users' usage of features and functionality ("Usage data").
- user actions such as logins, changes and deletion of data

For purposes of clarity, Usage Data excludes all data processed on the Applications. Veriforce will own and retain all right, title, and interest in and to the Usage Data and may use Usage Data during and after the term of the contracted services for the purposes of implementing, operating, maintaining and improving the Applications and fulfilling its obligations hereunder.

This information is used to:

- keep track of account changes
- maintain the Applications (fixing errors, clearing disputes etc)
- investigate any issues, service requests, bugs, fixes etc
- maintain the security and operation of our services
- provide our services during the term of the Agreement and during and after the term of the Agreement to create statistical analyses
- support our research and product development efforts

- for internal analytics and reporting purposes
- understand how you're using our Application and services so that we can continue to provide the best experience possible

Some of this information may also be collected using cookies; see Cookies section below.

The information we collect includes:

Log and Usage Data. Log and usage data is service-related, diagnostic, usage, and performance information our servers automatically collect when you access or use our services and which we record in log files. Depending on how you interact with us, this log data may include your Internet Protocol addresses, device information, browser type, and settings and information about your activity in the services (such as the date/time stamps associated with your usage, pages and files viewed, searches, and other actions you take such as which features you use), device event information (such as system activity, error reports (sometimes called "crash dumps"), and hardware settings).

Device Data. We collect device data such as information about your computer, phone, table, or other device you use to access the services. Depending on the device used, this device data may include information such as your Internet Protocol address or proxy server), device and application identification numbers, location, browser type, hardware model, Internet service provider and/or mobile carrier, operating system, and system configuration information.

Location Data. We collect location data such as information about your devices/location, which can be either precise or imprecise. How much information we collect depends on the type and settings of the device you use to access the services. For example, we may use GPS and other technologies to collect geolocation data that tells us your current location (based on your Internet Protocol address). You can opt out of allowing us to collect this information either by refusing access to the information or by disabling your location setting on your device. However, if you choose to opt out, you may not be able to use certain aspects of the services.

How we use your personal information

We rely on one or more of the following:

- **Consent:** We may process your personal information after you have consented (agreed) to us doing so. Your consent may have been obtained by us, or by third parties on our behalf. You have the right to withdraw your consent at any time.
- **Contract:** We may process your personal information when we need to deliver a contractual service to you or because you have asked us to do something before entering into a contract (e.g., provide a quote).
- **Legal obligation:** We may process your personal information when we need to comply with a legal obligation.
  Legitimate interest: We may process your personal information when we need to for our or another's legitimate interests, where these interests are not overridden by your rights.

We may use your personal information we collect for one or more of the following purposes:

- To provide you with information, products or services that you request from us, including processing of payments. For example, if you provide us with personal information in order for us to register you into a webinar, we will use that information to enroll and give you access to the webinar;
- To enhance our Applications and services and develop new ones. For example, by tracking and monitoring your use of Applications and services so we can keep improving or by carrying out technical analysis of our Applications and services so that we can optimise your user experience and provide you with more efficient tools;
- To conduct due diligence, including verifying your identity, as well as your eligibility to receive information, products, or services (such as verifying age, employment, or account status);
- To provide you with email alerts, event registrations and other notices concerning our products or services, or events or news, that may be of interest to you;
- To send transactional communications (such as requests for information, responses to requests for information, orders, confirmations, training materials, technical support issues and service updates) whether by email, by phone or otherwise;
- To carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collections;
- To create a database of Certified Customers which can be accessed by our clients;
- To process and acknowledge any job application that you may make;
- To complete risk management and mitigation activities, including for audit and insurance functions, and as needed to license and protect intellectual property and other assets;
- For testing, research, analysis, product development and to carry out various analysis and gather metrics related to our performance of our services and interactions with you in order to deliver enhanced services to you;
- To carry out market research about our products and services and to understand our customer base;
- For business activities, management reporting, and analysis, development, analytics, and business intelligence;
- As necessary or appropriate to protect the rights, property or safety of us, our Customers or others and to ensure security of our Applications and services, including monitoring individuals with access to the websites, applications, systems, or facilities, investigation of threats, and as needed for any data security breach notification;
- To protect ourselves and you through detection and prevention of any fraudulent or malicious activity and to make sure that everyone is using our Applications and services fairly and in accordance with our Terms of Service and End User License Agreement/Acceptable Use Policy available on our platform and or website.

- For relationship management and marketing. This purpose includes sending marketing and promotional communications to individuals who have not objected to receiving such messages, such as product and service marketing communications, customer communications (e.g., product updates, and training opportunities and invitations to Veriforce events), customer satisfaction surveys, supplier communications (e.g., requests for proposals), corporate communications, and Veriforce news. Please note you may unsubscribe at any time, by clicking the unsubscribe link in the email.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations;
- As described to you when collecting your personal information or as otherwise set forth in the applicable privacy legislation;
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by us is among the assets transferred.
- Additionally, Veriforce uses your Personal Data for secondary purposes such as: (i) disaster recovery and business continuity; (ii) internal audits or investigations; (iii) implementation or verification of business controls; (iv) statistical, historical, or scientific research; (v) dispute resolution; (vi) legal or business counseling; (vii) compliance with laws and company policies; and/or (viii) insurance purposes.
- To protect our services. We may process your information as part of our efforts to keep our services safe and secure, including fraud monitoring and prevention.

We will not use your personal information for automated decision making or profiling.

How we share your information

We do not generally share your personal information but if we need to, we will only disclose your personal information to:

- Our Affiliates. These are companies that are under the same common ownership as Veriforce. They include, but not limited to ComplyWorks Canada, ComplyWorks South Africa, and CHAS 2013 Limited.
- Employers. Authorized account administrators of Suppliers and Users accounts may authorize the sharing of the account profile and information with Clients in our Applications database for marketing and networking purposes.
- Third party service providers and partners who assist and enable us to maintain the Applications and carry out our services, for example:
    - to support delivery of or provide functionality on the Applications or services,
    - to provide IT managed services and server hosting services
    - to provide telephony services, or

    - to market or promote our Applications and services to you
    - facilitation and administration of the Common Assessment Standard
- Regulators, law enforcement bodies, government agencies, courts or other third parties where it's necessary to comply with applicable laws or regulations or to exercise, establish or defend our legal rights. Where possible and appropriate, we will notify you of this type of disclosure
- An actual or potential buyer (and its agents and advisors) in connection with an actual or proposed purchase, merger or acquisition of any part of our business

Veriforce does not sell personal information.

How we store your personal information and for how long

Your personal information is stored on the Applications servers in Canada and the USA.

Some of our third-party service providers are based in the USA and other international jurisdictions. We conduct Risk assessments on all suppliers and have Data Processing agreements in place with all to ensure private data is processed appropriately and safely.

The length of time we keep your personal information depends on whether we have an ongoing business need to retain it (for example, to provide you with a service you've requested, to comply with applicable legal, tax or accounting requirements or to comply with our contractual obligations with Clients and Suppliers).

We'll retain your personal information for as long as we have an ongoing relationship with you and for a period of time afterwards where there is an ongoing business need to retain it. Following that period, we'll make sure it's deleted or anonymized.

Security and confidentiality

Veriforce has implemented commercially reasonable and appropriate technical, physical, and organizational measures to protect the personal information from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition, or access during the processing to meet the requirements of applicable legislation.

Your rights

It's your personal information and you have certain rights relating to it. When it comes to marketing communications, you can ask us not to send you these at any time by following the unsubscribe instructions contained in the marketing communications.

Based on the country you live in, you may also have the following rights:

Your right of access - You have the right to ask us for copies of your personal information. You may also access your personal information by logging into the Applications.

Your right to correct or rectify - You have the right to request us to correct, update or rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure/deletion/to be forgotten - You have the right to request erasure/deletion of your personal information, subject to our regulatory and contractual obligations.

Your right to restriction of processing - You have the right to request us to restrict the processing of your personal information under certain circumstances.

Your right to object to processing - You have the right to object to the processing of your personal information under certain circumstances.

Your right to data portability - You have the right to request that we transfer the personal information you provided us, to another organisation, or to you, under certain circumstances.

Your right to withdraw consent – You have the right to withdraw consent regarding our collection and use of any of your personal information that was collected based on your previous consent at any time.

You are not required to pay any fees for exercising your rights. If you make a request, we have a fixed period of time, depending on the applicable privacy legislation, within which to respond to you. We will keep you updated of the progress of your request, as well as of the final result.

For individuals based in the United States

If you are a resident of the USA, you may be granted specific rights regarding access to and use of your personal information depending on the state you are a resident of.

Notwithstanding the fact that this Privacy Policy has references to the privacy laws specific to California, we ensure compliance with all applicable state-specific privacy regulations and laws, including those, not specifically mentioned herein.

California privacy legislation requires us to provide specific language and form, and since other state-specific privacy regulations have the same level of protection, but do not require the specific language or form, all other US jurisdictions are covered by CCPA Privacy Notice.

For individuals based in California

CCPA Privacy Notice

Veriforce has operations in California and is subject to California privacy laws.

This Privacy Policy and the sections above explain what personal information we collect and how we treat it for all jurisdictions, including California. This section displays the same information in the format required by California privacy laws.

Veriforce collects the following categories of personal information.

We collect information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer, household, or device (“personal information”). Personal information does not include:

- Publicly available information from government records.
- Deidentified or aggregated consumer information.
- Information excluded from the CCPA's scope, like:
    - health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA), clinical trial data, or other qualifying research data;
    - personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

In particular, we have collected the following categories of personal information from consumers within the last twelve (12) months:

Category	Data that may be collected	Collected
A. Identifiers	**Name, contact information, online identifiers, Social Security Numbers and other government-issued ID numbers, telephone numbers, email address, Internet Protocol address, account name, unique personal identifier. (on clients' instructions)**	**Yes**
B. Personal Information, as defined in the California consumer records law	**Name, contact information, insurance policy number, education, employment, employment history**	**Yes**
C. Protected classification characteristics under California or federal law	**Sex, age, race, color, religion or creed, ancestry, national origin, disability, medical conditions, genetic information AIDS/HIV status, marital status, sexual orientation, gender identity, citizenship, primary language, immigration status, military/veteran status, political affiliation/activities, domestic violence victim status, and request for leave.**	**Yes (to the extent the data is requested to be collected by the customer)**

D. Commercial information	**Transaction information, purchase history and financial details**	**Yes**
E. Biometric information	**Fingerprints and voiceprints**	**No**
F. Internet or other similar network activity	**Browsing history, search history, online behavior, interest data, interactions with our websites, applications, systems, advertisements**	**Yes**
G. Geolocation data	**Device location**	**Yes**
H. Audio, electronic, visual, thermal, olfactory, or similar information	**Images and audio, video or call recordings created in connection with our business activities**	**No (Unless the individuals participate in recorded meetings or calls)**
I. Professional or employment-related information	**Business contact details, work history, prior employments, human resources data and data necessary for benefits and related administrative services, professional qualifications, job titles**	**Yes**
J. Education Information	**Student records and directory information**	**No**
K. Inferences drawn from other personal information	**Inferences drawn from any of the collected personal information listed above to create a profile or summary about, for example and individual's preferences, abilities, aptitudes and characteristics**	**Yes**
L. Sensitive	**Social security numbers, account login**	**Yes (to the**

Personal Information	**information, contents of email or text messages, debit or credit card numbers, drivers' licenses, precise geolocation and state ID card numbers**	**extent the data is requested to be collected by the customer)**

We will use and retain the collected personal information as needed to provide the services or for Categories A, B, C, D, F, G, H, I, K, L for 7 years or longer if required by applicable legislation.

Category L information may be used or disclosed to a service provider or contractor, for additional, specified purposes. You have the right to limit the use or disclosure of your sensitive personal information.

We may also collect other personal information outside of these categories through instances where you interact with us in person, online, or by phone or mail in the context of:

- Receiving help through our customer support channels;
- Participation in customer surveys or contests; and
- Facilitation in the delivery of our services and to respond to your inquiries.

Use of personal information

We may use your personal information we collect for one or more of the following purposes:

- To provide you with information, products or services that you request from us, including processing of payments. For example, if you provide us with personal information in order for us to register you into a webinar, we will use that information to enroll and give you access to the webinar;
- To enhance our Applications and services and develop new ones. For example, by tracking and monitoring your use of Applications and services so we can keep improving or by carrying out technical analysis of our Applications and services so that we can optimise your user experience and provide you with more efficient tools;
- To conduct due diligence, including verifying your identity, as well as your eligibility to receive information, products, or services (such as verifying age, employment, or account status);
- To provide you with email alerts, event registrations and other notices concerning our products or services, or events or news, that may be of interest to you;
- To send transactional communications (such as requests for information, responses to requests for information, orders, confirmations, training materials, technical support issues and service updates) whether by email, by phone or otherwise;

- To carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collections;
- To complete risk management and mitigation activities, including for audit and insurance functions, and as needed to license and protect intellectual property and other assets;
- For testing, research, analysis, product development and to carry out various analysis and gather metrics related to our performance of our services and interactions with you in order to deliver enhanced services to you;
- To carry out market research about our products and services and to understand our customer base;
- For business activities, management reporting, and analysis, development, analytics, and business intelligence;
- As necessary or appropriate to protect the rights, property or safety of us, our customers or others and to ensure security of our Applications and services, including monitoring individuals with access to the websites, applications, systems, or facilities, investigation of threats, and as needed for any data security breach notification;
- To protect ourselves and you through detection and prevention of any fraudulent or malicious activity and to make sure that everyone is using our Applications and services fairly and in accordance with our terms and conditions available on our platform.
- For relationship management and marketing. This purpose includes sending marketing and promotional communications to individuals who have not objected to receiving such messages, such as product and service marketing communications, customer communications (e.g., product updates, and training opportunities and invitations to Veriforce events), customer satisfaction surveys, supplier communications (e.g., requests for proposals), corporate communications, and Veriforce news. Please note you may unsubscribe at any time, by clicking the unsubscribe link in the email.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations;
- As described to you when collecting your personal information or as otherwise set forth in the CCPA;
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by us is among the assets transferred;
- To detect and prevent security incidents;
- To debug to identify and repair errors;
- To perform services such as maintaining accounts, providing customer service and fulfill orders;

- To undertake internal research;
- To verify or maintain quality or safety of a service or device;
- Additionally, Veriforce uses your Personal Data for secondary purposes such as: (i) disaster recovery and business continuity; (ii) internal audits or investigations; (iii) implementation or verification of business controls; (iv) statistical, historical, or scientific research; (v) dispute resolution; (vi) legal or business counseling; (vii) compliance with laws and company policies; and/or (viii) insurance purposes.

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Sources of personal information

Veriforce collects this personal information actively (e.g. direct input from you) or passively (e.g. website cookies). Additionally, we may also collect personal information from our Customers, Employers, business partners and vendors, where applicable.

More information about our data collection and sharing practices can be found in this privacy notice.

You may contact us by email at privacy@veriforce.com, by calling toll-free at 1 (800) 673-1283, by visiting URL, or by referring to the contact details in the "How to Contact Us" Section.

Sharing personal information

We may disclose your personal information to a third party for a business purpose. When we disclose personal information for a business purpose, we enter into a contract that describes the purpose and requires the recipient to keep that personal information confidential and not use it for any purpose except in compliance with the contract.

Please note that we do not sell personal information for any monetary consideration, and we do not engage in any cross-context behavioral advertising towards any consumers. We use B2B marketing strategies (such as account-based marketing) to generate sales leads; however, the use of personal information in connection with these marketing efforts, based on our analysis, does not qualify as a "sell" or "share" under the CCPA.

In the preceding twelve (12) months, we have disclosed the following categories of personal information for a business purpose:

Personal Information Category	**Business Purpose of Disclosure**
A. Identifiers	➢ **Service providers for cloud services, software development, IT and system administration, internal audit functions,**

	quality assurance, customer support, document review services, maintenance services, other administrative and processing services, and professional services ➢ **Compliance platform** ➢ **Communication tool providers** ➢ **Data analytics providers** ➢ **ID verification providers** ➢ **CRM providers** ➢ **Marketing service providers** ➢ **Suppliers and Customers in the network of the Services who you work with or seek to work with through our Services**
B. Personal Information, as defined in the California consumer records law	➢ **Service providers for cloud services, software development, IT and system administration, internal audit functions, quality assurance, customer support, document review services, maintenance services, other administrative and processing services, and professional services** ➢ **ID verification providers** ➢ **Suppliers and Customers in the network of the Services who you work with or seek to work with through our Services**
C. Protected classification characteristics under California or federal law	➢ **Service providers for cloud services, software development, IT and system administration, internal audit functions, quality assurance, customer support, document review services, maintenance services, other administrative and processing services, and professional services**

	➢ **Compliance platform** ➢ **ID verification providers** ➢ **Suppliers and Customers in the network of the Services who you work with or seek to work with through our Services**
D. Commercial information	➢ **Service providers for cloud services, software development, IT and system administration, internal audit functions, quality assurance, customer support, document review services, maintenance services, other administrative and processing services, and professional services** ➢ **Compliance platform** ➢ **ID verification providers** ➢ **Suppliers and Customers in the network of the Services who you work with or seek to work with through our Services**
E. Biometric information	**Not collected**
F. Internet or other similar network activity	➢ **Service providers for cloud services, software development, IT and system administration, internal audit functions, quality assurance, customer support, document review services, maintenance services, other administrative and processing services, and professional services** ➢ **Compliance platform** ➢ **Communication tool providers** ➢ **Data analytics providers** ➢ **ID verification providers** ➢ **CRM providers**

	➢ **Marketing service providers** ➢ **Suppliers and Customers in the network of the Services who you work with or seek to work with through our Services**
G. Geolocation data	➢ **Service providers for cloud services, software development, IT and system administration, internal audit functions, quality assurance, customer support, document review services, maintenance services, other administrative and processing services, and professional services** ➢ **Compliance tool providers** ➢ **Communication tool providers** ➢ **Data analytics providers** ➢ **ID verification providers** ➢ **CRM providers** ➢ **Marketing service providers** ➢ **Suppliers and Customers in the network of the Services who you work with or seek to work with through our Services**
H. Audio, electronic, visual, thermal, olfactory, or similar information	➢ **Service providers for cloud services, software development, IT and system administration, internal audit functions, quality assurance, customer support, document review services, maintenance services, other administrative and processing services, and professional services** ➢ **Communication tool providers**
I. Professional or employment-related information	➢ **Service providers for cloud services, software development, IT and system administration, internal audit functions,**

	quality assurance, customer support, document review services, maintenance services, other administrative and processing services, and professional services ➢ **Compliance tool providers** ➢ **ID verification providers** ➢ **Suppliers and Customers in the network of the Services who you work with or seek to work with through our Services**
J. Education Information	**Not collected**
K. Inferences drawn from other personal information	**Not collected**
L. Sensitive Personal Information	➢ **Service providers for cloud services, software development, IT and system administration, internal audit functions, quality assurance, customer support, document review services, maintenance services, other administrative and processing services, and professional services** ➢ **Compliance tool providers** ➢ **Communication tool providers** ➢ **ID verification providers** ➢ **CRM providers** ➢ **Suppliers and Customers in the network of the Services who you work with or seek to work with through our Services**

We disclose your personal information for a business purpose to the following categories of third parties:

- Our affiliates at Veriforce may share personal information between and among Veriforce, its subsidiaries, and affiliated companies for purposes of management and analysis, and other business purposes.
- Service providers. The personal information is provided in order for them to provide Veriforce with services such as payment processing, data processing, IT services, customer support and other services such as auditing and fraud investigations. These subcontractors have access to your personal information only for the purpose of performing services on our behalf and are expressly obligated not to disclose or use your personal information for any other purpose.
- Law enforcement and other authorities. Veriforce may be required to disclose your personal information to third parties including law enforcement agencies when required to protect and defend our legal rights, protect the safety and security of End Users of our Applications and services, prevent fraud, respond to legal process, or a request for cooperation by a government entity, as required by law.
- In the event of sale, transfer, merger, reorganization, or similar event Veriforce may transfer your personal information to one or more third parties as part of that transaction with the business entities or people involved in the deal negotiation or transfer.
- Veriforce may share personal information about you with other third-parties if you give us permission or direct us to share the information. For example, when you appoint authorized agents to communicate with us.

In the preceding twelve (12) months, we have not sold any personal information.

Retention of personal information:

Veriforce retains the personal information during the duration of the contractual relationship under which the personal information was collected and for a fixed period of time afterwards. The retention period is determined by contractual obligations and regulatory requirements applicable to each type of personal information. We will retain your personal information for as long as reasonably necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal information for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you. To determine the appropriate retention period for personal information, we consider the amount, nature and sensitivity of the personal information, the purposes for which we process your personal information and applicable legal, contractual and regulatory requirements. In some circumstances we will anonymize your personal information for statistical purposes, in which case we may use this information indefinitely without further notice to you.

Disclosures related to sensitive personal information:

Veriforce may collect the following types of personal sensitive information from its individual Customers:

- Social security numbers, driver's license, state identification card, or passport number;
    - Purpose for collection: verification of identification as required by regulatory requirements
- Log-in details for their accounts in the Applications, debit card or credit card number combined with any required security or access code, password or credentials allowing access to an account;
    - Purpose for collection: authentication and authorization to access the Applications
- Precise geolocation;
    - Purpose for collection: information acquisition about current customers, enhance user experience, conduct targeted advertising campaigns, marketing efforts budget planning

The sensitive personal information is shared with Veriforce Affiliates for the purpose of maintenance of the data and Applications, and fulfilling our contractual obligations.

Veriforce does not sell sensitive personal information.

California Privacy Rights

If you are a California resident and are engaged in a business relationship directly with Veriforce for the provision of Veriforce services or products, you may request the following information from Veriforce.

1) Right to Know – You may request that we disclose to you the categories of, and specific pieces of personal information that we collected about you for the 12-month period preceding your request, including:
    - The categories of personal information we collected about you,
    - The categories of sources from which we collected such personal information;
    - The purpose for collecting personal information about you; and
    - The categories of third parties with access to your personal information, if any.
2) Right to Request Deletion of your personal information – You may request that we delete your personal information that we have collected from you or maintain about you, subject to certain regulatory exceptions (e.g. if we are required by law to retain the information).
3) Right to Opt-Out of Sale of personal information Veriforce does not sell the personal information it collects from its Customers, Employers and End Users.

4) Right to Non-Discrimination – We will not discriminate against any consumer who has chosen to exercise their rights under the CCPA (i.e. deny you or charge you different prices/rate for products or services or provide you different levels of quality of service).

5) Right to limit the use of sensitive personal information - Veriforce does not use your sensitive personal information for purposes that are not necessary to perform the services contracted to deliver to you.

6) Right to correct inaccurate information - You have the right to ask us to correct or modify the personal information we have about you.

7) Right to opt-out of automated decision-making technology - Veriforce does not use automated decision-making technologies.

Limit the Use of Sensitive Personal Information

You have the right to direct that we limit the use of your sensitive personal information to that use which is necessary to perform the services.

Once we receive your request, we are no longer allowed to use or disclose your personal information for any other purpose unless you provide consent for the use or disclosure of sensitive personal information for additional purposes.

Please note that sensitive personal information that is collected or processed without the purpose of inferring characteristics about you is not covered by these rights, as well as the publicly available information.

To exercise these rights, you can contact us by email at privacy@veriforce.com, by calling toll-free at 1 (800) 673-1283, by visiting “Do Not Sell or Share my Personal Information/Limit the Use of Sensitive Personal Information”, or by referring to the contact details in the “How to Contact Us” Section.

Sale of Personal Information

We do not engage in the sale of personal information as contemplated by the CCPA. As outlined in this Privacy Policy we do share personal information with other businesses for product, services and advertising reasons, however we do not share personal information for the purpose of receiving compensation for that information.

Please refer to California Consumer Rights Request Form if you want to exercise any of your rights under the CCPA, including the right to opt-out of the “sale” of your personal information and limit the use of sensitive personal information.

How to submit a California Rights Request

If this Privacy Statement applies to you, you may make a request for the disclosures described above or make a request to delete personal information we collected from you. See section “How to contact us” below for further details.

Verification process

Upon receipt of your request, we will provide directions on identity verification requirements which may include your name, email address and/or information Veriforce maintains on you, where appropriate. Your request will not be processed until your identity has been verified.

These verification efforts require us to ask you to provide information so that we can match it with information you have previously provided us with. For instance, depending on the type of request you submit, we may ask you to provide certain information so we can match the information you provide with the information we already have on file, or we may contact you through a communication method (e.g. phone or email) that you have previously provided to us. We may also use other verification methods as the circumstances dictate.

We will only use personal information provided in your request to verify your identity or authority to make the request. To the extent possible, we will avoid requesting additional information from you for the purposes of verification. However, if we cannot verify your identity from the information already maintained by us, we may request you provide additional information for the purposes of verifying your identity and for security of fraud-prevention purposes. We will delete such additionally provided information as soon as we finish verifying you.

Once your identity has been confirmed, your request will be processed in accordance with the CCPA.

Authorized Agents Submitting a Rights Request on Behalf of a Consumer

You may choose to designate an authorized agent to make a request under the CCPA on your behalf. No information will be disclosed until the authorized agent's authority has been reviewed and verified. Once a request has been submitted by an authorized agent, we may require additional information (i.e. your written authorization) to confirm the authorized agent's authority.

Other Privacy rights

- You may object to the processing of your personal information.
- You may request correction of your personal data if it is incorrect or no longer relevant, or ask to restrict the processing of the information
- You can designate an authorized agent to make a request under the CCPA on your behalf. We may deny a request from an authorized agent that does not submit proof that they have been validly authorized to act on your behalf in accordance with the CCPA.
- You may request to opt out from future selling or sharing of your personal information to third parties. Upon receiving an opt-out request, we will act upon the request as soon as feasibly possible, but no later than forty-five (45) days from the date of the request submission.
- To exercise these rights, you can contact us by email at privacy@veriforce.com, by calling toll-free at 1 (800) 673-1283, by visiting "Do Not Sell or Share my Personal Information/Limit the Use of Sensitive Personal Information", or by referring to the contact details in the "How to Contact Us" Section.

- California's "Shine the Light" law (Civil Code Section § 1798.83) permits users of our Services that are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. To make such a request, please send an email to privacy@veriforce.com.

Metrics

Under the CCPA, any business that processes the personal information of 10 million or more California residents annually, is required to disclose metrics about data subject access requests from California residents for the previous calendar year.

We do not process the personal information of 10 million or more California residents annually.

Sub-processors

We have implemented a Vendor Management Procedure and perform risk assessments on all new and existing vendors to ensure the vendors meet the information security and privacy requirements. A list of all vendors and third parties that are engaged in data sub-processing is kept updated and are available to Customers at https://veriforce.com/subprocessors.

All sub-processors are contractually bound to uphold the same level of information security and data privacy as we have in place.

How to Contact Us

Please contact us for more information or if you have questions or comments about our general privacy practices at privacy@veriforce.com. You may also reach us by mail at the address below. If you send us a letter, please provide your name, address, email address, and detailed information about your question, comment, or complaint and relationship with us.

1575 Sawdust Road, Suite 600,

The Woodlands, Texas 77380, US

1 (800) 673-1283 (Toll-free 24/7 privacy line)

For individuals based in European Union, EEA, Switzerland and UK

For listing of which countries are in the EU or EEA see https://europa.eu/european-union/about-eu/countries_en#other-european-countries and https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:European_Economic_Area_(EEA).

The information below should be read in addition to the information in the section "**What information we collect and how**", **"How we use your personal information**

How we share your personal information", **"How we store your personal information and for what time period**", **"Your rights**".

Veriforce acts as a processor of your personal data collected for the purpose of providing the functionality of the Applications and associated services to Customers and Employers. We only process personal data as instructed or permitted by our Customers and Employers. The Customers and Employers are controllers of the personal data.

We have appointed an EU and UK representative, DataRep, which you may contact, should you have a complaint, comment or request:

- sending an email to DataRep at datarequest@datarep.com quoting “Veriforce Inc” in the subject line or
- completing the online webform at www.datarep.com/data-request

International Data Transfers

We collect and process your personal data in the USA and Canada. We also share your personal data with service providers, affiliates and other third parties based in the USA and other jurisdictions without adequacy status. See section “How we share your information” above.

For data processing in USA and other non-adequacy countries, we have implemented an approved transfer mechanism in place to protect your personal data through the use of contractual agreements incorporating the European Commission’s Standard Contractual Clauses.

Data Privacy

For the purpose of the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council (“EU GDPR”), the United Kingdom General Data Protection Act (“UK GDPR”), and other applicable data protection laws with a framework similar to the EU GDPR, we are a “data processor” for your personal data when the processing is carried out on behalf our customers (such as processing of your personal data contained in the prequalification forms), and is a “data controller” when the processing is for our own purposes (such as billing, account management, product development, and other legitimate business interests. We are a processor and not a controller of Customers data. We only process data on instruction from Customers and process the data as per contractual agreement with the Customer. Veriforce will never sell or distribute or make private or Customer data available. Veriforce has implemented a Global Data Privacy Programme that is rolled out across all operations and has been designed to comply with multiple jurisdictional requirements. A Privacy Policy sets out the rights and obligations around this matter. We are compliant with GDPR requirements and have DPA’s and standard contractual clauses in place where required. Customers own their data and the data is only kept as long as is legally or contractually required. Users and Customers can request to have personal data corrected or removed at any time.

We have implemented a Vendor Management Procedure and perform risk assessments on all new and existing vendors to ensure the vendors meet the information security and privacy requirements. A list of all vendors and third parties that are engaged in data sub-processing is kept updated and are available to Customers at https://veriforce.com/subprocessors.

How to contact us

If you would like to get in touch with us with any privacy related questions/comments or if you would like to exercise your rights, we have appointed and EU and UK representative, DataRep, which you may contact, should you have a complaint, comment or request:

Contact us at privacy@veriforce.com or write to our Data Protection Representative at:

- sending an email to DataRep at datarequest@datarep.com quoting “Complyworks ltd” in the subject line or
- completing the online webform at www.datarep.com/data-request

We will get back to you within regulatory timelines.

If you are located in the EU, you also have a right to contact your local data protection authority as related to any of our privacy practices. Here is a list of EU data protection authorities and their addresses https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en.

Please note this is an external website over which we have no control; pls check their Privacy Policy to understand what personal information they collect and how they use it.

Your Right to Lodge a Complaint with the ICO - If you have a complaint about the way we are handling your personal information or think we have not complied with our obligations under data protection law, you may contact the Information Commissioner’s Office (ICO), which is the supervisory authority (regulator) in the UK.

You may make a complaint to the IC as follows;

Online: https://ico.org.uk/make-a-complaint

Live chat: https://ico.org.uk/global/contact-us/live-chat

Tel: 0303 123 1113.

Please note you should raise your complaint with the ICO within three months of your last meaningful contact with us.

For individuals based in Canada

The information below should be read in addition to the information in the section “**What information we collect and how**”, **“How we use your personal information**

How we share your personal information”, **“How we store your personal information and for what time period**”, **“Your rights**”

We process your personal information as per requirements of the federal Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) and Alberta PIPA.

Your rights to your personal information are:

Right to access

- If you have access to the Applications, you may access your personal information by logging into your user account. You may also request information and/or a copy of your personal information by contacting us.
- If you do not have access to the Applications, you may contact us at privacy@veriforce.com to obtain more information about what personal information we have and also to obtain a copy of their personal information.

Right to be informed

- You have a right to be informed of our privacy practices. This Privacy Policy is providing the required notice of what personal information we collect, how we use it and who we share it with.

Right to rectification

- You may contact us to request correction of the personal information stored in the Applications, if you believe it is inaccurate or incomplete.

Right to deletion

- You may have the right to request deletion of your personal information. This right is subject to contractual obligations between us and our Customers and Employers as well as to other legal requirements. This means that we may not be able to delete your personal information. We will inform you of the result of your request.

How to contact us

If you would like to get in touch with us with any privacy related questions/comments or if you would like to exercise your rights, contact us at privacy@veriforce.com or write to us at:

4838 Richard Rd SW Suite 200,

Calgary, AB T3E 6L1, Canada

Privacy Complaints

You also have the right to complain to the federal or provincial Privacy Commissioners.

Here are the details:

Privacy Commissioner of Canada, 112 Kent Street, Ottawa, Ontario, K1A 1H3 -or- to the Office of the Information

For contact information for all provincial privacy commissioners or ombudsman, see https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/

Cookies Section

Cookies are small text files that are placed on your computer by websites that you visit.

Our Applications use cookies to:

- manage user access,
- store user preferences,
- protect the website and manage network resources and traffic, and
- support the live chat functionality

See the Cookies banner for more information.