StarCompliance

Privacy Policy

February 14th 2024

Table of Contents

What is this?

This policy explains when and why we process personal data collected from you or provided to us from third parties, and how this data is used, the conditions under which it will be disclosed to others and how we secure your data. This policy also informs you of your rights you may have in respect of processing your personal data.

This policy will be updated from time to time in accordance with changing privacy and data protection laws and regulations. If these changes have any impact on the way we process your personal data – this policy will say so.

Who we are

StarCompliance is a leading provider of employee compliance software that protects the world's most reputable companies against risk and costly conflicts of interest.

We help clients around the globe streamline and automate their compliance programs. The StarCompliance technology was developed with the modern compliance team in mind, empowering organizations to achieve regulatory compliance while safeguarding their business reputation and saving time and resources.

StarCompliance is a data controller regarding all employee data and all marketing data. We are a data processor regarding client data.

Information that you give us

You give us information about yourself when you make an enquiry to StarCompliance or engage us to provide a service to you, or when entering information via our website, opt in/consent forms, apps or by communicating with us by phone, post, email, social media or through employment agencies or direct to StarCompliance recruitment, or otherwise. It includes additional information that you provide to us during the course of any business.

Information we receive from you or other third parties

Category	Data included in this category
Contact details	Name, email address, mobile number, company address.
Identification Information	Name, email address, mobile number, date of birth, passport details, home address.
Financial or billing	Bank account number, bank account name, bank account sort code. Company name
Employment information	Previous employers, C.V. required references
Emails	Contents of emails, email addresses of sender & receiver, colleagues that are CC'd into the emails.
Marketing databases	Name email addresses, job titles, mobile phone numbers, employer name and location.
While at work	Face/image voice, written messages. Meeting participation. Recordings of meetings that you have participated.
HR data	Name address, personal email address, contact phone number, name and address of next of kin. Previous employment details, details of individuals that have supplied an employment reference. Passport details. Selective health information. Background verification screening Information. Educational information.

The above details could be shared with us by employment agencies who have a copy of your CV.

The personal data we collect

Visitors to the StarCompliance website, offices, public and private events can be asked to provide personal data relating to:

Category	Personal data included in this category
Queries and or feedback	Name, email address, telephone number
Email alerts	Name, email address
Access to our website	Website navigation, whether you open items and which links you click on, cookie use page tagging techniques
Your internet protocol (IP)	IP address, web browser you use.

Information we automatically collect about you

We may automatically collect information about you which we may observe, detect or create without directly asking you to provide the information to us. This is in common with most other businesses, this will mainly include information gathered automatically through the use of our website or online services. The settings on our website allows you to reject the non-essential cookies.

How and why we use your personal data

We may use your personal data we collect about you in the following ways:

Where it is necessary to perform a contract with you:

- We will use and process your data where we have supplied you (or continue to supply you) with any StarCompliance services.
- Where you are in discussions with us about a particular matter on which you are considering taking our services.
- We will use your information in connection with the contract for the provision of services when it is needed to carry out that contract for you to enter into it.
- We may also use and process your personal data in connection with our recruitment activities. If you apply for a position with us (whether directly or through a third party) or send us your details on a speculative basis.

Where we have Legitimate Interest

- To verify the accuracy of data that we hold on you and to create a better understanding of you as a client.
- To create a profile of you based on any preferences you have indicated to us to enable us to decide what products and services to offer to you for marketing purposes
- To inform you about relevant events, products, news updates and announcements you may be interested in.
- To manage and deliver internal projects for business improvements
- For network and information security purposes to enable us to take steps to protect your personal data against loss or damage, theft or unauthorized access.
- To comply with you in connection with the exercising of your rights (if you ask us not to contact you, we will keep you on our suppression list in order to comply with your request)
- To assist in the management of requests or queries and complaints
- For the establishment, exercise or defense of our legal rights.

Our work for you may require us to provide information to third parties who will use your information for the purposes of providing services to us or directly to you on our behalf. These third parties may include payment processing, software providers, marketing services, professional, customer or technical services, data center providers and/or cloud service providers.

When we use these third parties, we only supply the personal information that is required for them to perform the service. We have contracts in place with such third parties to ensure your data is secure and protected. And to ensure that it is not used for any other purpose. These contracts are reviewed on an annual basis.

We may transfer your data if we are under a duty to disclose or share it in order to comply with any legal obligations, or to detect or report a crime.

Categories of individuals whose data we may collect

Categories of individuals	
Employees	Employees (past and present) includes permanent and contracting staff, part time and full time staff.
Non Employees	Non employees, assignees, advisors, consultants and other professional experts, secondments, interns and all other third parties.
	Job applicants, candidates, and pre hires
	Client contact, current and past contacts and prospects – including employees, officers, agents, consultants and other professional experts.
	Vendor, supplier contacts.

	Members of the press and other organizations. Members of charities. Regulators, business intermediates.
	Website users and complainants, correspondence and enquirers.
	Individuals attending StarCompliance events.
	Shareholders.
	Other Third parties.

Categories of data we may process

Categories of personal data	
Personal details	Name, all types of contact details, email, phone numbers, home landline. Place of work number, mobile number. Gender, date of birth, place of birth, nationality identification number, social security number, internal employee number or ID numbers. Marital status, domestic partners, dependents, disability status, emergency contacts details, such as names and addresses, phone numbers of listed individual. Ethnic origin, country of residence. Photographic image. CCTV or other video systems. Metrics systems used for data analytics, driver license number car details, passport number details contained in letters of application and CV. Background screening/vetting checks. eLearning and training programs, internal/external qualifications, performance and development reviews.
Personal details – clients and prospects.	Name, email, phone numbers, home landline. Place of work number, mobile number. Contact preferences, preferred medium for communication. Marketing preferences, data relating to services provided. Place of work. Relationship with StarCompliance representative, data related to event.
Personal details, vendors service providers suppliers, payees	Name, all types of contact details, such as title, job title, email, all categories pf phone numbers home and work address. Data related to invitations for business events. Bank details, invoicing address. Company registration numbers, company VAT numbers. Any type of unique identification numbers. Details of relationship to StarCompliance.
Other Individual	Name, all types of contact details, such as title, job title, email, all categories of phone numbers home and work address. Contact preference. Data relating to interaction or relationship to StarCompliance.

Documents required under immigration law	Citizens passport data details of residency, work permits.
Compensation and payroll	Renumeration details, tax codes, insurance codes, statutory and voluntary contributions, overtime and shift work. Compensation type, pay frequency, salary reviews. Performance reviews, bank details, credit card details. Working time records. Pay data, expense details, receipts from expenses.
Leaves of absence	Annual leave requests and approvals, statutory leave (maternity and paternity) Data relating to administrative leave (suspension), illness, leave due to accident at work. Occupational health leave (in accordance with local law). Dates of all the above listings.
Pension records	Monthly, yearly pension capital sums, deferred pension sums. Type of pension.
Position	Description of current position, job title, corporate status, career level, job function. Legal employment entity. Location of work, employee identification number, terms of employment, contract of employment. Length of service. Promotion prospects. Disciplinary records.
Work location	Work address and location. Employment permits visa expiry dates.
Management records	Details of any shares of common stock or directorships. Stock purchases, plans purchase eligibility and contribution. Stock options and information.
Marketing	Promoting and providing products and services to actual and potential customers, advertising marketing and PR related activities.
Accounts and records data. Data relating to vendors, service providers, suppliers' payees and intermediaries legal service data	Bank account details, including banking institution and bank account number, account balances and financial assets. Personal securities trading data. Details of personal securities transactions carried out by the data subject or on their retrospective behalf.
Data relating to mergers. Ventures and acquisitions	Management and employment information. Compensation and payroll details. Client relationships. Compliance due diligence. Full company reporting; finance and legal. Risk management, corporate audits.

Your rights

You have a number of rights in relation to your personal data under the Data Protection legislation. In relation to those rights, we may ask you for information to confirm your identity, and where applicable, or clarification to enable us to find your personal data. Except in rare cases, we will respond to you within one month from either:

(1) the data that we have confirmed your identity or
(2) where we do not need to do this because we already have this information, from the date we received your request**.**

Where we act as the processor of your data, we will contact the data controller. The data controller is responsible for responding to subject access requests. As a processor we have contractual arrangements in place to define the procedure.

Accessing your personal data

You have the right to ask for a copy of the data we hold about you by emailing us or writing to us at the address at the end of this policy. We may not provide you with a copy of your personal data if it contains information on other individuals, or we have another reason to withhold the data. We may charge you a reasonable fee based on administrative costs if you request a copy of data we have previously provided to you or if your request is excessive. We will try to provide you with a copy of your data electronically, unless you specify otherwise within your original request.

Correcting and updating your personal data

The accuracy of your data is important to us, therefore if you change your name or address/email address, or you discover that any of the other data we hold is inaccurate or out of date, please let us know by contacting us using the details set out at the end of this policy.

Withdrawing your consent

Where we rely on your consent as the lawful basis for processing your personal data, you may withdraw your consent at any time by emailing us or writing to us using the address at the end of this policy. If you withdraw your consent, our use of your data prior to this notification- the processing is still lawful.

Objecting to our use of your persona data

Where we rely on legitimate interest as the lawful basis for processing your data for any purpose, you may object to us using your personal data for these purposes by emailing us or writing to us, using the contact details at the end of this policy.

You may also object to us using your personal data for direct marketing purposes and we will immediately comply with your request.

Erasing your personal data or restricting its processing

In certain circumstances, you may ask for your personal data to be removed from our systems. Please note that, providing we do not have any continuing lawful reason to continue to process or hold your data, or if other exception noted in applicable privacy legislation, we will make all reasonable efforts to comply with your request.

Transferring your personal data in a structured data file

Where we rely on your consent as the lawful basis for processing your personal data or need to process it in connection with your contract, you may ask us to provide you with a copy of that data, in a structured data file. We will provide this to you in a structured commonly used and machine readable format.

Security

The transmission of information via the internet is not completely secure. While we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our website, and any transmission is at your own risk. Once we have received your personal data, we have in place reasonable and appropriate industry best practice controls to ensure that it remains secure against accidental or unlawful destruction, loss, alteration, or unauthorized access. All data is encrypted at rest and in transit.

Cookies

Like many other websites, StarCompliance uses cookies, cookies are small pieces of information sent to your computer and stored on its hard drive to allow our website to recognize you when you visit. You can switch these off by using the settings in your browser. For cookies used within our website, please follow this link; https://www.starcompliance.com/cookie-list Cookies are also used within our products, please see the below chart;

Cookies in use with StarCompliance products

Name of Cookie	Use of Cookie
.ASPXAUTH	Used to determine if a user is authenticated (removed on time /logout)
ASP.NET_SessionId	Used to identify the users session on the server (removed on time /logout)

SAML_SessionId	Used to identify the users SAML session on the server (removed on time /logout
__AntiXsrfToken	Cookie used to prevent Cross Site Request Forgery attacks (removed on time /logout)
MFATRUST	used when MFA is enabled for Forms Authentication (removed after the period set in a setting)
token	Cookie is used for authenticating requests to the backend from the frontend.
Csrftoken	Cross site request forgery protection
sessionid	To maintain the users session state
session	To maintain the users session state in airflow
requestedUri	Uri requested, helps the application UI with routing in a multi-tenant context
tenantName	Name of the users tenant
authRedir	To assist with redirect to authentication challenge if necessary
Optanon cookies	Cookie consent
https://www.starcompliance.com/cookie-list	For all cookies used on the marketing pages.

Transfer of personal data to a third party

We use third party providers to process your personal data. If we transfer data with third parties, we do this using the mechanism of Standard Contractual Clauses. This is a set of contractual clauses that ensure appropriate data protection safeguards are used for data transfers from the EU/UK to another country outside this area, where an adequacy decision is not in place.

Prior to any transfers, we conduct a privacy impact assessment.

Where we store our data

Region	Primary	Secondary
European Union Hosting	Azure West Europe, Amsterdam	Azure North Europe. Dublin, Ireland.
	Digital Reality Amstel Business Park HJE Wenckebachweh 127, 1096 Amsterdam. Netherlands.	Azure France Central. Paris, France
United Kingdom	Azure UK South. London	Azure UK West. Cardiff.

United States	Azure East US, Virginia, Unites States	Azure West US, California
United States	QTS Data Center, Dulles, VA	Azure West US 2. Quincy, WA
Canada Hosting	Azure Canada Central. Toronto, Ontario.	Azure Canada East. Quebec City. Quebec.
United Arab Emirates.	Azure UAE North. Dubai.	Azure UAE North. Dubai.

California Consumer Privacy Act.

Effective Date: As of January 1, 2023

This California Privacy Notice ("**Notice**") supplements, for California residents with which we interact in the business-to-business context ("**B2B Context**") as well as our job applicants, current employees, former employees, or independent contractors with which we interact in the human resources context ("**HR Context**") (collectively referred to throughout this Notice as "**you**" or "**your**"), the general privacy policies of StarCompliance Operating LLC (together with its relevant subsidiaries, associates, and affiliated companies, "**StarCompliance**," "**Company**," "**our**," "**us**," or "**we**"), including, without limitation, our Website Privacy Policy above and any other privacy policies, notices, or statements providing on a website, mobile app, or any other digital assets that we own and operate.

In the event of a conflict between any other Company policy, notice, or statement and this Notice, this Notice will prevail to California residents unless stated otherwise. You have certain privacy rights under the California Consumer Privacy Act, as amended by the California Privacy Rights Act, including the regulations promulgated thereunder (together, the "**CCPA**"). This Notice is designed to meet our obligations under the CCPA and provides information regarding our data practices, including our collection, use, disclosure, and Sale of your personal information ("**PI**"). Capitalized terms used but not defined in this Notice shall have the meanings given to them under the CCPA.

Applicability

- Section 1 of this Notice provides notice of our data practices, including our collection, use, disclosure, and Sale/Sharing of your PI.
- Sections 2-5 of this Notice provide information regarding your rights and how you may exercise them.

Non-Applicability, Customer Information

This Notice does not apply to information uploaded or imported into our systems, or otherwise provided to us to process, by customers in connection with the use of StarCompliance products and services ("**StarCompliance Customers**"). Any processing by StarCompliance of such information is governed by our services agreements with our customers. Please note that we are a service provider for StarCompliance Customers as we collect and process PI at the direction of StarCompliance Customers. If you have any questions about how the StarCompliance Customer has directed us to process your PI, please contact the applicable StarCompliance Customer.

Notice of data practices

The description of our data practices in this Notice covers the twelve (12) months prior to the Effective Date. Our data practices may differ between updates, however, if materially different from this Notice, we will provide supplemental pre-collection notice of the current practices, which may include references to other privacy policies, notices, or statements. Otherwise, this Notice serves as our notice at collection.

Personal Information and how we use your information

We may Collect your PI directly from you such as when you fill out the contact us form on our website or when you apply for a position or become employed or engaged by us (e.g., identification/identity data, contact details, educational and employment data); your devices; our affiliates; service providers; public sources of data; credit reporting agencies; third parties (e.g., references), or other businesses or individuals.
Generally, we Process your PI to provide you services and as otherwise related to the operation of our business, including for one or more of the following Business Purposes: Performing Services; Managing Interactions and Transactions; Security; Debugging; Advertising & Marketing; Quality Assurance; Processing Interactions and Transactions; and Research and Development.

- For example, in the course of you interacting with us on behalf of the business for which you work, we may use PI for the following purposes:
- Performing services;
- Communicating about our services;
- Advertising our products and services;
- Processing requests;
- Invoicing and collections activities;
- Enabling features on our website;
- Detecting security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted PI;
- Verifying or maintaining the quality or safety of our products or services; and
- Improving, upgrading, or enhancing our products and services.

For example, in the HR context we may use PI for the following purposes:

- Recruitment;
- Running background checks;
- Employee intake/ onboarding/ off-boarding;
- Maintaining personnel records;
- Payroll, reimbursements, and timekeeping;
- Processing leaves of absence;
- Processing workers' compensation claims;
- Booking employee travel;

- Benefits administration;
- Employee activation initiatives and communications;
- Facilitating diversity and inclusion programs;
- Administering training and education programs;
- HR IT systems and security;
- Employee and performance management;
- Health & safety/occupational health; and
- Security (including electronic and of premises)

We may also use PI for "**Additional Business Purposes**" in a context that is not a Sale or Share under the CCPA, such as:

- Disclosing it to our Service Providers, Contractors, or Processors that perform services for us ("Vendors");
- Disclosing it to you or to other parties at your direction or through your actions (e.g., payroll processors, benefits providers, some software platform operators);
- For the additional purposes explained at the time of collection (such as in the applicable privacy policy or notice);
- As required or permitted by applicable law;
- To the government or private parties to comply with law or legal process or protect or enforce legal rights or obligations or prevent harm;
- Where we believe we need to in order to investigate, prevent or take action if we think someone might be using information for illegal activities, fraud, or in ways that may threaten someone's safety or violate our policies or legal obligations; and
- To assignees as part of an acquisition, merger, asset sale, or other transaction where another party assumes control over all or part of our business ("Corporate Transaction").

Subject to restrictions and obligations under the CCPA, our Vendors may also use your PI for Business Purposes and Additional Business Purposes, and may engage their own vendors to enable them to perform services for us.

We may also use and disclose your PI under this Notice for Commercial Purposes, which may be considered a "Sale" or "Share" under the CCPA, when Third-Party Digital Businesses (defined below) Collect your PI via third-party cookies, and/or when we Process PI for certain advertising purposes, such as:

- Targeting advertisements to you or your device;
- Ad measurement, attribution, and other ad administration;
- Sending targeted ads on social media and other platforms; and
- Creating targeted advertising segments.

(a) Personal information, collection, disclosure, and retention

Categories of individuals whose data we may collect	Examples of data we collect	Categories of recipients	Why we collect it
Identifiers	Real name, alias, postal address, unique personal identifiers, online identifier, Internet Protocol address, e-mail address, and account name.	**Disclosures for Business Purposes**: • Vendors (e.g., web hosting and data analytics providers, processing and storage providers, fraud prevention and security providers, marketing services providers, and employment verification providers, benefits and payroll providers, learning management software providers); • Governmental entities (making requests pursuant to legal or regulatory process); and/or • Other parties within the limits of Additional Business Purposes. **Sale/Share**: Third-Party Digital Businesses	B2B Context HR Context
Personal Records	Name, signature, description, address, and telephone number. Some PI included in this category may overlap with other categories	**Disclosures for Business Purposes**: • Vendors (e.g., web hosting and data analytics providers, processing and storage providers, fraud prevention and security providers, marketing services providers, employment verification providers, benefits and payroll providers, learning management software providers); • Governmental entities (making requests pursuant to legal or regulatory process); and/or • Other parties within the limits of Additional Business Purposes. **Sale/Share**: None	B2B Context HR Context
Personal Characteristics or Traits	Gender, nationality, race or information related to medical conditions.	**Disclosures for Business Purposes**: • Vendors (e.g., processing and storage providers, fraud prevention and security providers, benefits and payroll providers); • Governmental entities (making requests pursuant to legal or regulatory process); and/or • Other parties within the limits of Additional Business Purposes.	HR Context

		Sale/Share: None	
Customer Account Details/ Commercial Information	Records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	**Disclosures for Business Purposes**: • Vendors (e.g., web hosting and data analytics providers, processing and storage providers, fraud prevention and security providers, marketing services providers, and benefits and payroll providers); • Governmental entities (making requests pursuant to legal or regulatory process); and/or • Other parties within the limits of Additional Business Purposes. **Sale/Share**: None	B2B Context HR Context
Internet Usage Information	When you browse our sites or otherwise interact with us online, we may Collect browsing history, search history, and other information regarding your interaction with our	**Disclosures for Business Purposes**: • Vendors (e.g., web hosting and data analytics providers, processing and storage providers, fraud prevention and security providers, and marketing services providers); • Governmental entities (making requests pursuant to legal or regulatory process); and/or • Other parties within the limits of Additional Business Purposes. **Sale/Share**: Third-Party Digital Businesses	B2B Context HR Context
Geolocation Data	If you interact with us online we may gain access to the approximate, and sometimes precise, location of the device or equipment you are using.	**Disclosures for Business Purposes**: • Vendors (e.g., web hosting and data analytics providers, processing and storage providers, fraud prevention and security providers, and marketing services providers); • Governmental entities (making requests pursuant to legal or regulatory process); and/or • Other parties within the limits of Additional Business Purposes. **Sale/Share:** Third-Party Digital Businesses	B2B Context HR Context
Sensory Data	We may Collect audio, electronic, or similar information when such as when you contact us through our customer service line, support services, and video security recordings.	**Disclosures for Business Purposes**: • Vendors (e.g., web hosting and data analytics providers, processing and storage providers, and fraud prevention and security providers); • Governmental entities (making requests pursuant to legal or regulatory process); and/or • Other parties within the limits of Additional Business Purposes.	B2B Context HR Context

		Sale/Share: None	
Professional or Employment Information	Professional, educational, or employment-related information.	**Disclosures for Business Purposes**: • Vendors (e.g., employment verification providers, web hosting and data analytics providers, processing and storage providers, and fraud prevention and security providers, and benefits and payroll providers); • Governmental entities (making requests pursuant to legal or regulatory process); and/or • Other parties within the limits of Additional Business Purposes.	B2B Context HR Context
Non-public Education Records	Education records directly maintained by an educational institution or party acting on its behalf, such as transcripts.	**Disclosures for Business Purposes**: • Vendors (e.g., employment verification providers, processing and storage providers, and benefits providers); • Governmental entities (making requests pursuant to legal or regulatory process); and/or • Other parties within the limits of Additional Business Purposes. **Sale/Share**: None	HR Context
Inferences from PI Collected	Inferences drawn from PI to create a profile reflecting preferences, abilities, and aptitudes.	**Disclosures for Business Purposes**: • Vendors (e.g., web hosting and data analytics providers, processing and storage providers, fraud prevention and security providers, marketing services providers, benefits providers, employee performance assessment providers, and HR survey providers); • Governmental entities (making requests pursuant to legal or regulatory process); and/or • Other parties within the limits of Additional Business Purposes. **Sale/Share**: Third-Party Digital Businesses	B2B Context HR Context
Sensitive PI	Government Issued Identification Numbers (e.g., social security, driver's license, state identification card, or passport number	**Disclosures for Business Purposes**: • Vendors (e.g., processing and storage providers, fraud prevention and security providers, payment processors, employment verification providers, and benefits and payroll providers); • Governmental entities (making requests pursuant to legal or regulatory process); and/or • Other parties within the limits of Additional Business Purposes.	HR Context

		Sale/Share: None	
	Precise Geolocation (any data that is derived from a device and that is used or intended to be used to locate an individual w/in a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet)	**Disclosures for Business Purposes**: • Vendors (e.g., web hosting and data analytics providers, processing and storage providers, fraud prevention and security providers, and marketing services providers); • Governmental entities (making requests pursuant to legal or regulatory process); and/or • Other parties within the limits of Additional Business Purposes. **Sale/Share**: Third-Party Digital Businesses	B2B Context HR Context
	Sensitive Personal Characteristics (e.g., racial or ethnic origin, religious or philosophical beliefs, citizenship or immigration status, or union membership)	**Disclosures for Business Purposes**: • Vendors (e.g., processing and storage providers, fraud prevention and security providers, and benefits providers); • Governmental entities (making requests pursuant to legal or regulatory process);and/or • Other parties within the limits of Additional Business Purposes. **Sale/Share**: None	HR Context
	Communication Content (e.g., the contents of an individual's StarCompliance email account, other than where StarCompliance is the intended recipient of the communication)	**Disclosures for Business Purposes**: • Vendors (e.g., processing and storage providers and fraud prevention and security providers); • Governmental entities (making requests pursuant to legal or regulatory process); and/or • Other parties within the limits of Additional Business Purposes. **Sale/Share**: None	HR Context
	Health Information (PI collected and analyzed concerning an individual's health, medical history, mental or physical health, diagnosis/condition, and medical treatment)	**Disclosures for Business Purposes**: • Vendors (e.g., processing and storage providers and benefits providers); • Governmental entities (making requests pursuant to legal or regulatory process); and/or • Other parties within the limits of Additional Business Purposes. **Sale/Share**: None	HR Context

	Sexual Orientation (PI collected and analyzed concerning an individual's or sexual orientation	**Disclosures for Business Purposes**: • Vendors (e.g., processing and storage providers); • Governmental entities (making requests pursuant to legal or regulatory process); and/or • Other parties within the limits of Additional Business Purposes. **Sale/Share**: None	HR Context (for voluntary diversity program purposes only)

There may be additional information we Collect that meets the definition of PI under the CCPA but is not reflected by a category above, in which case we will treat it as PI as required, but will not include it when we describe our practices by PI category.

As permitted by applicable law, we do not treat Deidentified data or Aggregate Consumer Information as PI and we reserve the right to convert, or permit others to convert, your PI into Deidentified data or Aggregate Consumer Information, and may elect not to treat publicly available information as PI. We will not attempt to reidentify data that we maintain as deidentified.

Because there are numerous types of PI in each category of PI, and various uses for each PI type, our retention periods vary for each of the categories of PI described above. The length of time for which we retain each category of PI depends on the purposes for our collection and use and requirements pursuant to applicable laws. In no event do we retain your PI for any longer than reasonably necessary to achieve the purposes for which it was collected or processed, or as required by applicable law. The criteria used to determine the retention period of PI includes the nature and sensitivity of the PI, the potential risk of harm from unauthorized use or disclosure of the PI, as well as applicable laws (such as applicable statutes of limitation).

Your Rights and How to Exercise Them

As described below, subject to meeting the requirements for a Verifiable Consumer Request (defined below) and limitations permitted by applicable laws, we provide you the privacy rights described in this section.

To submit a request to exercise your privacy rights, or to submit a request as an authorized agent, use the rights California Resident Privacy webform here.

Please respond to any follow up queries we make.

Right to limit sensitive PI processing

With regard to PI that qualifies as sensitive PI under the CCPA, if you elect to provide us with that sensitive PI you will have consented to such processing. For California residents for whom we process sensitive PI in the B2B Context, we only process such sensitive PI for purposes that are exempt from consumer choice under the CCPA. For California residents for whom we process sensitive PI in the HR context, you can limit certain Sensitive PI Processing. If you do so we will explain in a response what processing purposes the CCPA do not allow you to limit.

Right to know/Access

You have the right to access your PI up to two times in any 12 month timescale. The PI you have access to is limited to:

- The categories of PI we have collected about you.
- The categories of sources from which we collected your PI.
- The business purposes or commercial purposes for our collecting, selling, or sharing your PI.
- The categories of third parties to whom we have disclosed your PI.
- A list of the categories of PI disclosed for a business purpose and, for each, the categories of recipients, or that no disclosure occurred.

A list of the categories of PI sold or shared about you and, for each, the categories of recipients, or that no sale or share occurred.

Specific Pieces

You may request to confirm if we are Processing your PI and, if we are, to obtain a transportable copy, subject to applicable request limits, of your PI that we have Collected and are maintaining. For your specific pieces of PI, as required by the CCPA, we will apply the heightened verification standards as described below. We have no obligation to re-identify information or to keep PI longer than we need it or are required to by applicable law to comply with access requests.

Do not sell/Share

California consumer privacy act, has an opt-out from selling and from sharing for cross-context behavioral advertising (use of PI from different businesses or services to target advertisements). We may sell or share your PI, as these terms apply under the CCPA. However, we provide you with an opt out of sale/sharing.

Third-Party digital businesses ("**Third-Party Digital Businesses**") may associate cookies and other tracking technologies that collect PI about you on our services, or otherwise collect and process PI that we make available about you, including digital activity information. We understand that giving access to PI on our services, or otherwise, to third-party digital businesses could be deemed a sale and/or share and thus we will treat such PI

(e.g., cookie ID, IP address, and other online IDs and internet or other electronic activity information) collected by third-party digital businesses, where not limited to acting as our service provider (or contractor or processor), as a sale and/or share and subject to a do not sell/share opt-out request. We will not sell or share your PI if you make a do not sell/share opt-out request.

Opt-out for non-cookie PI: If you want to opt-out of the sale/sharing of your non-cookie PI (e.g., your email address), make an opt-out request with the ''cookie setting'' on any page of the web site.

Opt-out for cookie PI: If you to opt-out of the sale/sharing of such PI, you need to exercise a separate opt-out request on our cookie management tool located in the bottom left corner on our website here. This is because we have to use different technologies to apply your opt-out of cookie PI and to non-cookie PI. Our cookie management tool enables you to exercise such an opt-out request and enable certain cookie preferences on your device. You must exercise your preferences on each of our websites and apps you visit, from each browser you use, and on each device that you use. Since your browser opt-out is designated by a cookie, if you clear or block cookies, your preferences will no longer be effective and you will need to enable them again via our cookie management tool. Beware that if you use ad blocking software, our cookie banner may not appear when you visit our services and you may have to use the link above to access the tool.

Opt-out preference signals (also known as global privacy control or "GPC"): The CCPA requires businesses to process GPC signals, which is referred to in CCPA as opt-out preference signals ("**OOPS**"), which are signals sent by a platform, technology, or mechanism, enabled by individuals on their devices or browsers, that communicate the individual's choice to opt-out of the Sale and Sharing of personal information. To use an OOPS/GPC, you can download an internet browser or a plugin to use on your current internet browser and follow the settings to enable the OOPS/GPC. We have configured the settings of our consent management platform to receive and process GPC signals on our website. We process OOPS/GPC with respect to Sales and Sharing that may occur in the context of Collection of cookie PI by tracking technologies online by Third-Party Digital Businesses, discussed above, and apply it to the specific browser on which you enable OOPS/GPC. We currently do not, due to technical limitations, process OOPS/GPC for opt-outs of Sales and Sharing in other contexts (e.g., non-cookie PI). We receive and process OOPS/GPC in a "frictionless manner," which means we do not: (1) charge a fee for use of our service if you have enabled OOPS/GPC; (2) change your experience with any product or service if you use OOPS/GPC; or (3) display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial in response to the OOPS/GPC.

We do not knowingly Sell or Share the PI of Consumers under 16, unless we receive affirmative authorization ("opt-in") from either the Consumer who is between 13 and 16 years old, or the parent or guardian of a Consumer who is less than 13 years old. If you think we may have unknowingly collected PI of a Consumer under 16 years old, please Contact us at info@starcompliance.com

We may disclose your PI for the following purposes, which are not a sale or share: (i) if you direct us to disclose PI; (ii) to comply with a rights request you submit to us; (iii) disclosures amongst the entities that constitute company as defined above, or as part of a corporate transaction; and (iv) as otherwise required or permitted by applicable law.

Right to delete

Except to the extent we have a basis for retention under applicable law, you may request that we delete your PI. Note also that, we may not be required to delete your PI that we did not collect directly from you.

(b) Correct Your PI

You may bring inaccuracies in the PI that we maintain to our attention and we will act accordingly. You can also make changes to your online account in the account settings section of the account. That will not, however, change your information that exists in other places.

Version control and amendments.

This policy will be reviewed on an annual basis or if there is a significant change to the data protection legislation. Please re visit this page from time to time to ensure you are happy with any changes we may make.

Contact Us

If you have any questions regarding your data and how we process it, please contact us.

By post; StarCompliance, Unit 1 Innovation Close, Heslington. York.

By email; info@starcompliance.com

If you are not happy with the contact you have received from StarCompliance, you have the right to contact the Supervisory Authority; In the United Kingdom this is the Information Commissioners Office. Tel 0303 123 1113.

Our European Supervisory Authority representation

By post: GRCI Law; Third Floor, The Boyne Tower, Bull Ring, Lagvooren, Drogheda, Co Louth, Ireland A92 F682.

By email: eurep@itgovernance.eu

By Telephone:+44 (0)333 900 5555

United States Of America

By post; 9200 Corporate Blvd, Suite 440, Rockville, MD 20850

Email: info@starcompliance.com