Privacy Policy

22nd May 2018

Classification: Public

Status: Approved

Version: 7

Table of Contents

Definitions 3
What this Privacy Policy covers 4
The Personal Data we collect 4
How Personal Data is used and for what purpose 5
Transfer of Personal Data to a Third Party 5
General Data Protection Regulation 5
Privacy Shield 5
How we maintain confidentiality, integrity and availability of your Personal Data 6
How we retain and destroy your Personal Data 6
Your individual rights in respect to your Personal Data 6
Subject Access Request 7
Personal Data of children under 13 years of age 7
Privacy Shield - Binding Arbitration 7
Monitoring of Internal Activities 8
Changes to this Policy 8
Contact details if you have any questions relating to the use of your Personal Data 8
Contact Us 9

Definitions

StarCompliance – StarCompliance, Inc. and any majority-owned or controlled subsidiaries or affiliates.

Solution - Means the StarCompliance regulatory compliance software solution.

Personal Data – Any information relating to an individual, including name, telephone number, address, email address, social security number, personal business transaction details, Account Information and Personal Trading Data.

Special Category Data – The processing of Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person sex life or sexual orientation.

Sensitive Personal Information - means government identification numbers or financial account numbers associated with individual persons (e.g. U.S. or U.K. Social Security numbers, driver's license numbers, or personal credit card or banking account numbers), and medical records or health care claim information associated with individuals, including claims for payment or reimbursement for any type of medical care for an individual.

Processing of personal information or "processing" – Any operation or set of operations performed on personal information, whether by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, combination, blocking, erasure or destruction.

Third Party – Any person, partnership, corporation, public authority, government agency, or any other entity other than the individual, under the direct authority of StarCompliance, that are authorized to process the data.

Recipient –The person, public authority, government agency, or any other entity to which Personal Data is disclosed, even if the recipient is a third party.

Data Controller - determines how and why Personal Data is processed. For more information, read the Cabinet Office's entry in the Data Protection Public Register.

Data Processor – is responsible for processing Personal Data on behalf of a Data Controller.

No distinction between "data" and "information" is made in this policy.

Overview

StarCompliance is a leading provider of compliance and regulatory solutions for financial services and enterprise firms. We provide compliance software with a focus on global regulations including, SEC, FINRA, FCPA, FCA, UK Bribery Act, and MiFID. Our solutions provide a fully configurable platform that manages the complex and burdensome processes associated with managing regulatory compliance, connecting all areas of your business and providing a 360-degree view of employee activity and behaviour.

StarCompliance offers products and services in the business-to-business market sector. StarCompliance operates as a Data Controller as an organization and a Data Processor in terms of its products and services for our Clients.

What this Privacy Policy covers

The StarCompliance Privacy Policy tells you what to expect when StarCompliance collects personal information from you in respect to:

- the Personal Data we collect;
- how Personal Data is used and for what purpose;
- the transfer of Personal Data to a Third Party;
- how we maintain accuracy, integrity and security of your Personal Data;
- how we retain and destroy your Personal Data;
- what are your individual rights in respect to your Personal Data;
- Personal Data of children under 13 years of age, and;
- contact details if you have any questions relating to the use of your Personal Data;

The Personal Data we collect

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

- queries or feedback you leave, including your name, email address, telephone number if you contact starcompliance.com;
- your name, email address and subscription preferences when you sign up to our email alerts;
- how you use our website - for example website navigation, whether you open items, and which links you click on, cookie use and page tagging techniques;
- Information provided to us in relation to technical assistance;
- StarCompliance product interactions and performance data in relation to our products and services, and;
- your Internet Protocol (IP) address, and details of which version of web browser you used.

How Personal Data is used and for what purpose

The Personal Data we collect is consistent with this Privacy Policy. Personal Data is used to provide and improve our products and services. The purpose of use may be based upon consent, legal obligation or legitimate interests, examples of these may include:

- Responding to Requests for Information;
- Responding to Subject Access Requests;
- Responding to Data Breach Notifications;
- Responding to Due Diligence requests;
- Providing audit evidence;
- Providing white papers and resources;
- Registering users for StarCompliance promotional material and events;
- Contacting users for marketing and sales queries;
- Evaluating and improving the online user experience;
- Compliance with legal, regulatory and business obligations

Transfer of Personal Data to a Third Party

StarCompliance does not sell, lease, rent or give away Personal Data. Personal Data is handled in line with StarCompliance Policies. Personal Data processed by StarCompliance is subject to:

General Data Protection Regulation

CHAPTER V TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS.

Privacy Shield

StarCompliance complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States, respectively. For purposes of enforcing compliance with the Privacy Shield, StarCompliance is subject to the investigatory and enforcement authority of the US Federal Trade Commission. For more information about Privacy Shield, see the US Department of Commerce's Privacy Shield website located at:

https://www.privacyshield.gov.

To review StarCompliance representation on the Privacy Shield list, see the US Department of Commerce's Privacy Shield self-certification list located at:

https://www.privacyshield.gov/participant?id=a2zt000000000rUAAQ&status=Active

Conflict between the terms in this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, please visit:

https://www.privacyshield.gov/.

StarCompliance adheres to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access and Recourse, Enforcement, and Liability.

How we maintain confidentiality, integrity and availability of your Personal Data

StarCompliance have made a commitment to the protection of all its informational assets, including Personal Data. The protection of informational assets, including Personal Data, relies upon the protection of the security principles:

- Confidentiality
- Integrity
- Availability

This is achieved through the application of the Security Controls: Administration, Technical and Physical. When combined these provide a number of security layers, designed to safeguard against any potential threats. These controls are subject to independent audits, security testing and external assessments by clients, and independent organizations against the latest industry standards.

These security controls require constant and consistent audits, reviews, monitoring and communication. This is provided by a Senior Management and Board through the practices of Governance, Risk and Compliance.

How we retain and destroy your Personal Data

StarCompliance is bound by legal regulatory and business obligations to the retention of Personal Data, in relation to:

- Maintaining business relationships;
- The provision of products, service or information based upon entitlement or reasonable expectations;
- Legal, regulatory, contractual compliance;

Please be aware that elements of legal and regulatory compliance may over-rule the fundamental rights associated with your data protection rights.

Destruction of Personal Data is subject to industry best practice.

Your individual rights in respect to your Personal Data

StarCompliance observes and upholds your rights in respect to the General Data Protection Regulation. These rights are based upon:

- the right to, request information regarding the Personal Data we process concerning you (Subject Access Request);
- the right to, rectify, update or complement inaccurate or incomplete Personal Data concerning you;
- the right to, delete or request the erasure of Personal Data concerning you, exceptions apply; for example, criminal records or due to legal and regulatory requirements;
- the right to, withdraw any consent you may have given for us to process Personal Data

concerning you;
- the right to object to our processing of Personal Data concerning you on the basis of our, or of third-parties' legitimate interests;
- the right to, obtain from us the portability of Personal Data concerning you which we process using automated means on the basis of your consent or of a contract you have entered into with us, and;
- the right to, in the European Economic Area, lodge a privacy complaint with a supervisory authority if you are unhappy with the way we have handled your Personal Data or any privacy query or request that you have raised with us.

Subject Access Request

A Subject Access Request is a request from an individual to see copies of information held by an organization about them, as such:

- StarCompliance is obliged to take reasonable measures to confirm your identity and the grounds of those making the request;
- StarCompliance will notify client-based requests (Subject Access Request) to the appropriate Data Controller within agreed timescales;
- StarCompliance will process other Subject Access Requests within one calendar month. This period is extendable under certain criteria.

Personal Data of children under 13 years of age

StarCompliance does not actively, or knowingly collect, process or store information from children under the age of 13.

Exception: employee dependencies based upon legal regulatory or contractual obligations, and or in relation to products, services or benefits.

Privacy Shield - Binding Arbitration

You may have the option to select binding arbitration for the resolution of your complaint under certain circumstances, provided you have taken the following steps:

- raised your complaint directly with StarCompliance and provided us the opportunity to resolve the issue;
- made use of the independent dispute resolution mechanism identified above; and
- raised the issue through the relevant data protection authority and allowed the US Department of Commerce an opportunity to resolve the complaint at no cost to you.

For more information on binding arbitration, see US Department of Commerce's Privacy Shield Framework: Annex I (Binding Arbitration):

https://www.privacyshield.gov/article?id=D-Binding-Nature-of-Decisions

Privacy Shield - Onward Transfer

In the context of an onward transfer, StarCompliance takes responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an

agent on its behalf. StarCompliance shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.

Monitoring of Internal Activities

StarCompliance does not engage in blanket monitoring of internal communications but does reserve the right to monitor access, retrieve, read, or disclose internal communications when:

- a legitimate business need exists that cannot be satisfied by other means;
- the involved individual is unavailable and timing is critical to a business activity;
- there is reasonable cause to suspect criminal activity or policy violation;
- monitoring is required by law, regulation, or third- party agreement.

At any time and without prior notice, StarCompliance management reserves the right to examine archived electronic mail, personal computer file directories, hard disk drive files, and other information stored on StarCompliance information processing systems. This information may include Personal Information. Such examinations are typically performed to assure compliance with internal policies, support the performance of internal investigations, and assist with the management of StarCompliance information processing systems.

Changes to this Policy

If StarCompliance seeks to make a material change to StarCompliance's policy to allow use of Personal Information for a new, legitimate business purpose, StarCompliance will document the change to this policy, note the date of the last update at the start of the policy, and publish the policy. You are encouraged to check this policy occasionally to stay informed of any changes in our policies and procedures regarding Personal Information. For substantial and material changes to this policy, StarCompliance will use reasonable efforts to provide notification to all affected users and suggest that such users review the updated policy.

Contact details if you have any questions relating to the use of your Personal Data

In compliance with the US-EU and Swiss-US Privacy Shield Principles, and the General Data Protection Regulations, StarCompliance commits to resolve complaints about your privacy and our collection or use of your personal information.

European Union or Swiss individuals with inquiries or complaints regarding this privacy policy should first contact the relevant Data Controller. Alternatively, you may also contact StarCompliance using the contact details below, if you have any questions about anything in this document, or you think that your Personal Data has been misused or mishandled.

US

StarCompliance - Information Security & Data Protection
Information Security Officer
451 Hungerford Drive, Suite 515, Rockville, MA 20580, USA
Office: +1 301-340-3900

UK

StarCompliance - Information Security & Data Protection
Information Security Officer
The Catalyst, Baird Lane, York, YO10 5GA, UK
Office: +44 (0)1904 300 887

Email: privacy@starcompliance.com

You can also report concerns to the Information Commissioner, who is an independent regulator:

https://ico.org.uk/concerns/

Contact Us

If you have any questions or queries, unrelated to this Privacy Policy, please contact StarCompliance with the details below:

T: +1 301-340-3900
F: +1 301-340-3906
E: info@starcompliance.com
W: www.starcompliance.com

451 Hungerford Drive, Suite 515,
Rockville, MD 20850, USA