DATA PRIVACY POLICY

Increasing the commercial value of your business relationships

Introduction

SCCI Ltd needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

Why this policy exists

This data protection policy ensures SCCI Ltd:

- Complies with data protection law and follows good practice
- Protects the rights of customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The GDPR/Data Protection Act 2018 describes how organisations including SCCI Ltd must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The Data Protection Act is underpinned by eight important principles. These say that personal data must be:

- Processed fairly and lawfully
- Obtained only for specific, lawful purposes
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Held for no longer than necessary
- Processed in accordance with the rights of data subjects
- Protected in appropriate ways

Policy scope

This policy applies to SCCI Ltd and all associates, contractors, suppliers and other people working on its behalf. It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR/Data Protection Act 2018. This can include:

- Names of individual
- Postal addresses
- Email addresses
- Telephone numbers

Plus, any other relevant information relating to individuals.

Data protection risks

This policy helps to protect SCCI Ltd from data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Registered in England No. 5150526

Responsibilities

Everyone who works for or with SCCI Ltd has responsibility for ensuring data is collected, stored and handled appropriately. All personal data must be handled and processed in line with this policy.

The board of directors is responsible for ensuring that SCCI Ltd meets its legal obligations:

- Keeping updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Dealing with requests from individuals to see the data SCCI Ltd holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails, letters, blogs and the company website.
- Ensuring marketing initiatives abide by data protection principles.

Data storage

These rules describe how and where data will be safely stored.

- Data in paper format will be kept in a secure place where unauthorised people cannot see it and will be shredded when no longer required.
- Data stored electronically will be protected from unauthorised access, accidental deletion and malicious hacking attempts:

Data use

- **Interviews & Surveys** - We handle both personally and commercially sensitive information. We, therefore, have a very strict information management and security policy. During appraisals, we guarantee that individual contributions are used without revealing sources and we do not retain names in our records beyond its end.
- **Mailing List** – We maintain a mailing list of individuals who have given us permission to periodically inform them of developments within the Collaboration field. They can unsubscribe from this service at any time.
- **Invoicing** – Customer details held in invoices are kept securely in accordance with accounting rules.
- **Business Cards** – We assume that when we are given business cards this implies permission to contact the donor and share the information freely with those people where there might be mutual benefit. We would use best intentions to ensure that the information is not misused.

Subject access requests

All individuals who are the subject of personal data held by SCCI Ltd are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, SCCI Ltd will disclose requested data and ensure the request is legitimate seeking assistance from legal advisers where necessary.

Date of Issue: 20 February 2023

For Further information contact:

Telephone: +44 1 908 561892
Email: sales@sccindex.com
Website: www.sccindex.com