Information Security Policy

Contents

Data Protection Policy

Context and overview

Key Details

- Policy prepared by: Caroline Thomas
- Approved by board / management: 3rd May 2022
- Policy became operational on: 3rd May 2022
- Next review by date: May 2023

Introduction

Social Accelerators Limited needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees, 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.

Privacy Statement

We respect your privacy and are committed to protecting your personal data.

This privacy statement will inform you as to how we look after your personal data and tell you about your privacy rights and how the law protects you. It also aims to give you information about how Social Accelerators Limited collects and processes your personal data.

This statement is not intended for children, and we do not knowingly collect data relating to children.

It is important that you read this privacy statement together with any other privacy notice or fair processing notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This privacy statement and data protection policy supplements the other notices and is not intended to override them.

Why this policy exists

This data protection policy ensures Social Accelerators:

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

Data protection law

Data Protection Act 2018

The Data Protection Act 2018 describes how organisations – including Social Accelerators 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 policy is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant, and not excessive
4. Be adequate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

People, risks, and responsibilities

Policy Scope

This Policy applies to:

- The head office of Social Accelerators
- All branches of Social Accelerators
- All staff and volunteers of Social Accelerators
- All Contractors, suppliers and other people working on behalf of Social Accelerators

It applies to all data that the company holds relating to identifiable individuals. This can include:

- Names of individuals
- Postal Addresses
- Email Addresses
- Telephone Numbers
- Usernames
- IP Addresses
- Organisations you may be employed by
- How you use our website and whether you open or forward our communication
- Sales information relating to purchases and services, including complaints.
- Plus any other information relating to the individuals.

- If you provide information on behalf of someone else, they must have given you permission to do so and have had sight of this data protection policy.

- We do not collect any Special Categories of Personal Data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

Data protection risks

This policy helps to protect Social Accelerators from some very real 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.

Responsibilities

Everyone who works for or with Social Accelerators has some responsibility for ensuring data is collected, stored, and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The board of directors is ultimately responsible for ensuring that Social Accelerators meets its legal obligations.

- The Data Protection Officer, Caroline Thomas, is responsible for:
    - Keeping the board updated about data protection responsibilities, risks, and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data Social Accelerators 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.
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.

- The IT manager, Robert Thomas, is responsible for:
    - 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.

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.

- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.

- Social Accelerators will provide training to all employees to help them understand their responsibilities when handling data.

- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

- In particular, strong passwords must be used and they should never be shared.

- Personal data should not be disclosed to unauthorised people, either within the company or externally.

- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

- All employees must explicitly agree to any personnel record checks including but not limited to criminal record checks to ensure the security of data processed by Social Accelerators.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

We aim to be paperless but when data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.

- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.

- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.

- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.

- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing services.

- Servers containing personal data should be sited in a secure location, away from general office space.

- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

- All servers and computers containing data should be protected by approved security software and a firewall.

Data use & Collection

Personal data is of no value to Social Accelerators unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.

- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.

- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.

- Personal data should never be transferred outside of the European Economic Area.

- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

- Protective Marking is applied to all files containing personal, sensitive and critical data to ensure it is marked as 'Restricted', 'Protect' or 'Not Protectively Marked', further to this the following protective marking is used to mark all files containing personal, sensitive and critical data as 'Commercial', 'Personal', 'Management'.

There are different ways in which data is collected from you and about you. You may give us your personal data by:

- filling in forms or by corresponding with us by post, phone, email or otherwise.
- This includes personal data you provide when you:
- Make an enquiry with us for one of our services
- Purchase a service or product
- Request marketing to be sent to you
- Enter a competition, promotion or survey; or
- Give us some feedback.
- Raise a ticket in our support system.
- Automated technologies or interactions. As you interact with our website, we may automatically collect data about your equipment, browsing actions and patterns.

Data accuracy

The law requires Social Accelerators to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Social Accelerators should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they make contact.

- Social Accelerators will make it easy for data subjects to update the information Social Accelerators holds about them. For instance, via the company website.

- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

- It is the Data Protection Officer's responsibility to ensure marketing databases are checked against industry suppression files every six months.

- Due to the nature of our business, we generally do not collect data from those aged sixteen (16) or under. If this was to occur any personal data collected on persons

under the age of sixteen (16) Social Accelerators will actively require parental consent to collect this data.

Subject access requests

All individuals who are the subject of personal data held by Social Accelerators 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.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller: Caroline Thomas caroline@socialaccelerators.com. The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will aim to provide the relevant data within one month.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Social Accelerators reserve the right to refuse or charge for requests that are manifestly unfounded or excessive.

If Social Accelerators refuse a request, Social Accelerators will tell the individual why and the individual has the right to complain to the supervisory authority and to a judicial remedy. Social Accelerators will do this without undue delay and at the latest, within one month.

Right to be forgotten

All individuals who are the subject of personal data held by Social Accelerators are entitled to:

- The right to erasure (right to be forgotten)

Any data subject has the right to obtain from the controller the erasure of personal data without undue delay. This can occur but not limited to:

The personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed.

The data subject withdraws consent, requests from individuals should be made by email, addressed to the data controller at Caroline Thomas caroline@socialaccelerators.com

Social Accelerators will within 30 days ensure any personal data held by Social Accelerators will be erased in adherence with the legal obligation in Union or Member State law to which the controller is subject.

The data controller will always verify the identity of anyone making a right to be forgotten request before erasing information.

If Social Accelerators refuse a request, Social Accelerators will tell the individual why and the individual has the right to complain to the supervisory authority and to a judicial remedy. Social Accelerators will do this without undue delay and at the latest, within one month.

Data Destruction

All data Social Accelerators hold will be securely irretrievably removed before disposal or shall be processed by a company that is accredited by ICER (Industry Council for Electronic Equipment Recycling) to recycle IT equipment and that will provide certification of destruction of data.

Data portability

Social Accelerators ensures the right of data portability.

Subject access requests allow for an individual to obtain their personal data held by Social Accelerators.

The processing and data is based inside the European Economic Area (EEA) this applies to both manual and automated methods.

If Social Accelerators refuse a request, Social Accelerators will tell the individual why and the individual has the right to complain to the supervisory authority and to a judicial remedy. Social Accelerators will do this without undue delay and at the latest, within one month.

Social Accelerators will ensure that the right of access needs to be balanced against other rights, such as intellectual property, trade secrecy and copyright protections for software

Disclosing data for other reasons

In certain circumstances, the law allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Social Accelerators will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Right to complain

Any individual who feels they have a problem in any way Social Accelerators have handled their data have the right to complain to the Information Commissioners Office.
https://ico.org.uk

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number.

A copy of our ICO registration is attached.

Providing information

Social Accelerators aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

Data breaches and intrusion

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the Social Accelerators becomes aware that a personal data breach has occurred, Social Accelerators will notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless Social Accelerators is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

Social Accelerators will communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication will describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects will be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

It is the responsibility of all directors and staff of Social Accelerators to report any suspected data breach or suspected intrusion to the relevant management as soon as feasibly possible. All suspected data breach or intrusion should be reported to the data protection officer Caroline Thomas to begin a full security incident report as per Social Accelerators security incident reporting documentation.

If a suspected data breach or intrusion is reported it shall be ascertained whether all appropriate technological protection and organisational measures have been implemented

to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The notification will be made without undue delay and taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject.

Technical Information

All devices including mobile devices used by Social Accelerators are under current support for security updates from manufacturers.

Wherever possible two factor authentication is in place and active.

Data stored on our Google account is encrypted at rest and during transit.

All data including our cloud and local devices has relevant backup systems in place.

Social Accelerators work closely with IT professionals who are available to provide assistance and guidance in relation to data protection.

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.org.uk

Certificate

Organisation Name:

The Social Accelerators Ltd

Reference number:

ZA318526

Tier:

Tier 1

Start date:

19 February 2018

End date:

18 February 2023

Data Protection Officer