Swiftium Data protection policy

Context and overview

Key details

- Policy prepared by Andrew Rinne
- Approved by board / management on: 04-15-2021
- Policy became operational on: 04-15-2021
- Next review date: 04-15-2022

Introduction

Swiftium, Inc. needs to gather and use certain information about individuals.

These individuals can include registrants at tradeshows where Swiftium, Inc. provides lead retrieval, ID badge, registration, equipment rental, or other services; customers, suppliers, business contacts, employees, and other people the organization 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 Swiftium, Inc.:

- Complies with data protection law and follows good practice.
- Protects the rights of staff, 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 Data Protection Act 1998 describes how organizations—including Swiftium—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:

1. Be processed fairly and lawfully.
2. Be obtained only for specific, lawful purposes.
3. Be adequate, relevant and not excessive.
4. Be accurate and kept up to date.
5. Not be held for any longer than necessary.
6. Be 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 Swiftium, Inc.
- All branches of Swiftium, Inc.
- All staff of Swiftium, Inc.
- All contractors, suppliers and other people working on behalf of Swiftium, Inc.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus, any other information relating to individuals.

Data protection risks

This policy helps to protect Swiftium, Inc. 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 Swiftium, Inc. 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 Swiftium, Inc. meets its legal obligations.

- The **Data Protection Officer, Pascal Abadie,** 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.

    - o Dealing with requests from individuals to see the data Swiftium, Inc. holds about them (also called *subject access requests*).
    - o Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The **CTO, Pascal Abadie,** is responsible for:
    - o Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - o Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - o Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

- The **Marketing Manager, Andrew Rinne,** is responsible for:
    - o Approving any data protection statements attached to communications such as emails and letters.
    - o Addressing any data protection queries from journalists or media outlets like newspapers.
    - o Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

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.

- **Swiftium, Inc. 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.

- Strong **passwords must be used,** and they should never be shared.

- Personal data **should not be disclosed** to unauthorized 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.

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.

When data is **stored on paper,** it should be kept in a secure place where unauthorized 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 unauthorized 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 unauthorized 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 **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 may optionally be stored on a mobile smartphone or tablet for usage with the Swiftium mobile apps. This data can be as little as a partial snapshot or full snapshot of an event's registration data. This data is encrypted using AES256 encryption standard and stored in a locked folder inaccessible to the user.

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

Data use

All data stored with the Swiftium; Inc. systems are for sole use of the data owner. Swiftium, Inc. never markets or distributes gathered data to anyone other than the data owner.

● The processing of personal data by Swiftium, Inc is carried out on behalf of Swiftium Clients and is described in the purchase order, statement of work, or written agreement signed by the parties' authorized representatives.

● Swiftium, Inc. receives personal data when exhibitors and attendees register for a tradeshow either through direct registration with Swiftium, Inc. or via API with a third party.

● For each lead retrieval event, the Swiftium, Inc. database is available to trade show exhibitors for 90 days after a event or other amount of time specified by the show organizer in written contract.

● Swiftium clients have access to and control of their own data for their events. Clients choose to store the data as long as they wish to and delete it when they wish to.

● Swiftium, Inc. doesn't own or control the any data gathered; the data belongs solely to client.

● 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.

Data accuracy

The law requires Swiftium, Inc. to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data be accurate, the greater the effort Swiftium, Inc. 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 call.

- Swiftium, Inc. will make it **easy for data subjects to update the information Swiftium, Inc.** holds about them. For instance, via email request.

- 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 marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Subject access requests

All individuals who are the subject of personal data held by Swiftium; Inc. 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 contact 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 at cust@Swiftium.com. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals are entitled to make a Subject Access Request free of charge. The data controller will aim to provide the relevant data within 10 business days.

Repeated Subject Access Requests by the same individual over a short period of time will be subject to a $25 administrative fee.

The data controller will always verify the identity of anyone making a Subject Access Request before handing over any information.

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, Swiftium, Inc. 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.

Providing information

Swiftium, Inc. 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.

Swiftium Rental Terms and Conditions

1. The RENTER shall keep and maintain the rented equipment during the terms of the rental at his own cost and expense. He shall keep the equipment in a good state of repair, normal wear and tear excepted.

2. The RENTER may choose to use their own shipping service to ship and insure equipment to and from the OWNER. RENTER may choose to use the OWNERS shipping service. Use of the OWNERS shipping service grants the OWNER the right to insure the shipment. The cost of shipping and insurance will be invoiced to the RENTER. The RENTER shall pay the OWNER full compensation for replacement and/or repair of any equipment which is lost, stolen, or damaged while the equipment is in the possession of the RENTER. Possession is defined as the rental period and the moment the equipment was delivered to the agreed upon address. The used shipping service account holder is responsible for filing a claim for compensation with the shipping service for lost/damaged/stolen equipment during transportation from the OWNER to the RENTER. RENTER shall pay for lost/damaged/stolen equipment during transportation from the RENTER to the OWNER.

3. Lost/damaged/stolen equipment cost varies depending on equipment rented from the OWNER. OWNER defines the cost of said equipment beyond the scope of this agreement. The return of previously lost/ stolen equipment constitutes a 90% refund

of the total returned equipment value to the RENTER from the OWNER. A 10% restocking fee is imposed on the refunded total.

4. The RENTER shall not remove the equipment from the address of the RENTER or the location shown herein as the place of use of the equipment without prior approval of the OWNER. The RENTER shall inform the OWNER upon demand of the exact location of the equipment while it is in the RENTERS's possession.

5. The equipment shall be delivered to RENTER and returned to OWNER at the RENTER's risk, cost and expense. If a periodic rental rate is charged by OWNER, rental charges are billed to the RENTER for each period or portions of the period from the time the equipment is delivered to RENTER until its return. If a term rental rate is charged by OWNER, rental charges are billed to the RENTER for the full term even if the equipment is returned before the end of the term. If the equipment is not returned during or at the end of the term, then the rental charges shall continue a full-term basis in addition to an exponentially increasing overage fee unless otherwise agreed upon by the OWNER.

6. No allowance will be made for any rented equipment or portion thereof which is claimed not to have been used. Acceptance of returned equipment by OWNER does not constitute a waiver of any of the rights OWNER has under the rental agreement. The OWNER permits a 10%consignment allowance of the total quantity ordered equipment to cover non-functioning equipment and/or additional equipment usage. Non- functioning equipment will not be invoiced to the RENTER. Additional equipment usage will be invoiced to the RENTER.

7. The RENTER shall not pledge or encumber the rented equipment in any way. The OWNER may terminate this agreement immediately upon the failure of RENTER to make rental payments when due, or upon RENTER's filling for protection from creditors in any court of competent jurisdiction.

8. RENTER indemnifies and holds OWNER harmless for all injuries or damage of any kind for repossession and for all consequential and special damages for any claimed breach of warranty.

9. The RENTER shall pay all reasonable attorney and other fees, the expenses and costs incurred by OWNER in protecting its rights under this rental agreement and for any action taken OWNER to collect any amounts due the OWNER under this rental agreement.

10. These terms are accepted by the RENTER upon delivery of the terms to the RENTER or the agent or other representative of RENTER.

11. The OWNER requires a 25% down payment on equipment orders exceeding 500 pieces upon agreement of the terms.

Swiftium Privacy Policy

Information we collect
In order to provide our service, the application collects information from machine-readable objects captured through voluntary use of the camera. Information about the device's cellular and wireless state is automatically collected in order to ensure a safe and secure transmission to our servers.

How this information is used
Information is transmitted via Secure Socket Layer (SSL) technology and stored for use by any license holder(s) of the data's originating application. Data is not shared with third parties except with the licensee's explicit consent.

Contacting Us
If there are any questions regarding this privacy policy, you may contact us using the information below.

494 N Middletown Rd, Pearl River, NY 10965
+1 201-735-0411 (Available 24/7)
Customer Support: support@Swiftium.com