EVENTSI tmi Petra Vairimaa

DATA PROTECTION POLICY

Policy Prepared and approved by
Petra Vairimaa
Policy become operational on
11.02.2018
Next review date 11.02.2019

Context and overview

Introduction

Eventsi is an event management company. In order to operate Eventsi 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.

Why this policy exists

This data protection policy ensures that Eventsi:

- Complies with data protection law and follow 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

REGULATION (EU) 2016/… OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

(General Data Protection Regulation)

describes how organisations — including Eventsi tmi— 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.

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of Eventsi tmi
- All branches of Eventsi tmi
- All staff and volunteers of Eventsi tmi
- All contractors, suppliers and other people working on behalf of Eventsi tmi

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
- Passport numbers
- …plus, any other information relating to individuals

Data protection risks

This policy helps to protect Eventsi tmi 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 Eventsi 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.

General staff guidelines

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

Data storage

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

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, DVD or external hard disk), 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.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

Personal data is of no value to Eventsi 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**.
- 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 Eventsi 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 Eventsi 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.
- 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.

Subject access requests

All individuals who are the subject of personal data held by Eventsi 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**.

Providing information

Eventsi 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.

Appendix 1

Description of the personal data management process in Eventsi

1) Eventsi can receive personal data from

a) client companies via email

b) directly from meeting participants via email

2) Eventsi stores and manages the personal data

a) during event creation and management process in

- Eventsi's employees PC's hard drive
- Eventsi's employees Smartphones
- Hard Copies
- Cloud Services (OneDrive via MS Office 365)

b) after the completion of an event

- data is stored in an external data storage, which is stored in a separate locked safe
- all the data from all above-mentioned devices and cloud locations is deleted after separately agreed timeframe with the client.
- all the hard copies containing personal data are destroyed

3) Eventsi can send personal data to the following entities:

a) Travel Company

b) Accommodation Company