Mirifique Events

Data Governance Policy

Policy overview

Mirifique Events is hereinafter referred to as "the company."

The company is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

The company needs to gather and use certain information about individuals. This can include customers, suppliers, business contacts, employees and other people the company 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 comply with the law.

Purpose of this policy

This data protection policy ensures the company:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is transparent about how it stores and processes individuals' data
- Takes reasonable steps to protect itself from the risks of a data breach

Data Protection Law

The Data Protection Act 1998 describes how organisations, including the company, 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. 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

Mirifique Events

Data Governance Policy

Policy Scope

This policy applies to the company, including all branches, employees, volunteers and all contractors, suppliers and other people working on behalf of the company where personal data is processed:

- In the context of the business activities of the company or any company entity.
- For the provision or offer of goods or services to individuals (including those provided or offered free-of-charge) by a company or company entity.
- To actively monitor the behaviour of individuals online.
- Monitoring the behaviour of individuals online includes using data processing techniques such as persistent web browser cookies or dynamic IP address tracking to profile an individual with a view to:
    - Taking a decision about them.
    - Analysing or predicting their personal preferences, behaviours and attitudes.

Personal data can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- And any other information relating to individuals

This policy applies to all Processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

Data protection risks

This policy helps to protect the company 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.

Responsibilities

The Directors are ultimately responsible for ensuring that the company meets its legal obligations. It is their responsibility for ensuring data is collected, stored and handled appropriately, including:

- Reviewing all data protection procedures and related policies.
- Arranging adequate data protection training and handling data protection questions for the people covered by this policy.
- Dealing with requests from individuals to see the data the company 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 and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- 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.
- The company will provide training to all employees to help them understand their responsibilities when handling data.
- All 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.

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

Data use

Personal data should be respected and protected from risk of loss, corruption and theft at all times. When using personal data you should ensure:

- 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 when containing sensitive information, as this form of communication is not secure.
- If personal data must be sent via email, it is good practice to encrypt that data before being transferred electronically. Data should also be encrypted where possible on all other electronic transfers.
- Personal data should never be transferred outside of the European Economic Area, with the exception to any trusted platforms (listed in Schedule 1) or third-parties (listed in Schedule 2) that operate in countries found by the EU Commission to have a 'positive finding of adequacy' or thats are signed up to the Safe Harbor Scheme, such as the United States, Canada or Australia.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data where possible.

Data accuracy

The law requires the company 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 the company should put into ensuring its accuracy.

Mirifique Events

Data Governance Policy

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.
- The company will make it easy for data subjects to update the information they hold 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.

Subject access requests

All individuals who are the subject of personal data held by the company 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 at info@mirifique.events . The data controller can supply a standard request form, although individuals do not have to use this.
- Subject access request information will be provided free of charge, unless the request is manifestly unfounded or excessive, for which a charge of £10 per subject access request will be made.
- The data controller will aim to provide the relevant data within 30 days.
- The data controller will always verify the identity of anyone making a subject access request before handing over any information.
- Within the process, the personal data should be provided from all systems listed in Schedule 1 and requested from all third-parties listed in Schedule 2.

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, the company 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 erasure ("right to be forgotten")

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

- Have their personal data erased.
- Make a request for erasure verbally or in writing.
- The data controller will aim to respond and action the request within 28 days.
- The data controller will always verify the identity of anyone making a subject access request before handing over any information.
- Within the process, the personal data should be deleted from all systems listed in Schedule 1 and requested from all third-parties listed in Schedule 2.

When does the right to erasure apply? Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

Providing information

The company 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.
- This is available on request and a version of the privacy policy statement is also available on the company's website

Mirifique Events

Data Governance Policy

Schedule 1

Systems operating by the company, which require a review for personal data requests to provide, update or delete their data:

- Gsuite for Business
- Mailchimp
- Facebook

Schedule 2

Trusted third-parties include:

- Your data is currently not shared with any trusted third-parties.