This policy describes how personal data must be collected, handled and stored to meet Rogue Fitness's data protection standards – and to comply with the law.

Data Protection Notice

Our Data Protection Notice

Introduction

Rogue Fitness needs to gather and use certain information about individuals.

These can include (current and former) 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 firm's data protection standards – and to comply with the law.

Why this policy exists

This data protection policy ensures Rogue Fitness:

- Complies with data protection law and follows good practice.
- Protects the rights of employees, 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 2018 and the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) describe how organisations – including Rogue Fitness – 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 2018 and General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) are 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

Policy Scope

This policy applies to:

- The head office of Rogue Fitness
- All remote locations of Rogue Fitness
- All employees and Partners of Rogue Fitness
- All contractors, suppliers and other people working on behalf of Rogue Fitness

It applies to all data that the firm holds relating to the identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). 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 Rogue Fitness 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 firm 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 Rogue Fitness 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 Partners are ultimately responsible for ensuring that Rogue Fitness meets its legal obligations.

The IT Manager is responsible for:

- Keeping the Partners updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from employees and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Rogue Fitness 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.

The Communications Manager is responsible for:

- Approving data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like
- Where necessary, working with other employees to ensure communications 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 direct managers.
- Rogue Fitness 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. Passwords need to be created in accordance with the password construction guidelines.
- Personal data should not be disclosed to unauthorised people, either within the firm 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 direct manager or the IT Manager 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.

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 and to original copies of documents:

- When not required, the paper or file 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.
-

- Paper Documents, especially originals of official purpose such as certificates or similar must be sent using tracked delivery services which obtain a signature upon delivery.
- Documents sent outside the remote workers country of origin should always be sent by a reputable international courier using tracked delivery services which obtain a signature upon delivery.

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

- All computers are required to have encrypted local disk drives in accordance with the acceptable encryption policy.
- Data should be protected by strong passwords that are changed regularly and never shared between employees. Passwords need to be created in accordance with the password construction guidelines.
- Data stored on USB drives, CD's or DVD's is not permitted. Any data sent to us in these formats should be given to IT for transfer to the correct secure storage location and the media should then be properly destroyed.
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service.
- 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 firm'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, anti-virus and a firewall.

Data Use

When personal data is accessed 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. 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 Rogue Fitness 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 Rogue Fitness 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 data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Rogue Fitness will make it easy for data subjects to update the information Rogue Fitness holds about them. For instance, via regular contact and review of data.
- 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 Communications manager's responsibility to ensure communications databases are checked against industry suppression files every six months.

Subject Access Rights

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

- Ask what information the firm 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 firm requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the IT manager at Info@RogueFitness.ie The data controller can supply a standard request form, although individuals do not have to use this.

Individuals may be charged €10 per subject access request. 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.

Disclosing Data for other Reasons

In certain circumstances, the Data Protection Act and the General Data Protection Regulation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Rogue Fitness will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Partners and from the firm's legal advisers where necessary.

Providing Information

Rogue Fitness 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 firm has a general privacy statement and specific privacy statements, setting out how data relating to individuals is used by the firm.

