Forth Estuary Forum Data Protection Policy

Approved by board of Directors on: 5th June 2018

Policy became operational on: 5th June 2018

Next review date: 01/05/2023

Introduction

The Forth Estuary Forum (or FEF) 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 the FEF:

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; and
Protects itself from the risks of a data breach.

Data protection law

The Data Protection Act 1998 and General Data Protection Regulation (GDPR) (EU) 2016/679 describe how organisations including the FEF 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:

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

Lawful Basis for Processing

The nature of business and actions conducted by FEF require that we process data under the following legal bases as set out in Article 6 of the GDPR:

Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

People, risks and responsibilities

This policy applies to:

The head office of FEF;
All staff and volunteers of FEF; and
All contractors, suppliers and other people working on behalf of FEF.

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 or General Data Protection Regulation (GDPR) (EU) 2016/679. This can include:

- Names of individuals;
- Postal addresses;
- E-mail addresses;
- Telephone numbers;
- Plus any other information relating to individuals.

Data protection risks

This policy helps to protect the FEF from some very real data security risks, including:

- Breaches of confidentiality, e.g: information being given out inappropriately;
- Failing to offer choice, e.g: all individuals should be free to choose how the company uses data relating to them;
- Reputational damage, e.g: the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with the FEF 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 the FEF meets its legal obligations.

The privacy monitoring shall be jointly shared between the Forum Manager and the Forum Administrator. Their responsibilities are detailed below.

The Forum Manager 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 the FEF holds about them (also called 'subject access requests'); and
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

The Forum Administrator 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;
- Approving any data protection statements attached to communications such as emails and letters; and
- Addressing any data protection queries from journalists or media outlets like newspapers.

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 FEF 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 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; and
- Employees should request help from their line manager if they are unsure about any aspect of data protection.

Data storage and Retention

A full set of Records Retention guidelines is available on the Forum Server as an appendix to this Data Protection Policy.

The following rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Forum 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:
    - 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, e.g. 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 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 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

Personal data is of no value to the FEF 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 e-mail, as this form of communication is not secure;
- Data must be encrypted before being transferred electronically;
- Personal data should never be transferred outside of the European Economic Area;
- Employees should not save copies of personal data to their own computers; and
- Always access and update the central copy of any data.

Data accuracy

The law requires the FEF 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 FEF 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, e.g: by confirming a customer's details when they call.

The FEF will make it easy for data subjects to update the information the FEF holds about them, e.g: *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.

Individual Rights

General Data Protection Regulation (GDPR) (EU) 2016/679 also guarantees individuals the following rights with regard to their personal information:

- Individuals have the right to be informed about the collection and use of their personal data;
- Individuals have the right to access their personal data and supplementary information;
- Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete;
- Individuals have the right to have personal data erased ('the right to be forgotten');
- Individuals have the right to request the restriction or suppression of their personal data. (This is not an absolute right and only applies in certain circumstances);
- Individuals have the right to obtain and reuse their personal data for their own purposes across different services;
- Individuals have the right to object to:
    - processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
    - direct marketing (including profiling); and
    - processing for purposes of scientific/historical research and statistics.

Subject access requests

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 e-mail, addressed to the data controller at secretary@forthestuaryforum.co.uk. The data controller can supply a standard request form, although individuals do not have to use this.

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, the FEF 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

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

- How the data is being used; and
- 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. A version of this statement is also available on the company's website www.forthestuaryforum.co.uk).

Appendix 1

Subject Access Request Form

This form should be used to request a Subject Access Request from the FEF as entitled under the Data Protection Act 1998. This form will identify:

- What information the FEF holds about the individual and why;
- Ask how to gain access to it;
- Be informed how to keep it up to date; and
- Be informed how the company is meeting its data protection obligations.

Please note, a subject access request from individuals should be made by email, addressed to the Forum at secretary@forthestuaryforum.co.uk.

The data controller will always verify the identify of anyone making a subject access request before handing over any information and you should send a scanned copy of formal ID such as drivers license or passport to confirm your identity. Failure to do so will result in the data controller either not proceeding with your subject access request or it being delayed.