Enterprise East Group C.I.C.

Data Protection Policy
GDPR

Privacy Notice

This is the privacy notice of Enterprise East Group CIC. In this document, "we", "our", or "us" refer to Enterprise East.

We are company number 0940814 registered in England and Wales.

Our registered office is at 82b High Street, Sawston, Cambridge, England, CB22 3HJ

Introduction

This privacy notice aims to inform you about how we collect and process any information that we collect from you, or that you provide to us. It covers information that could identify you ("personal information") and information that could not. In the context of the law and this notice, "process" means collect, store, transfer, use or otherwise act on information. It tells you about your privacy rights and how the law protects you.

We are committed to protecting your privacy and the confidentiality of your personal information. Our policy is not just an exercise in complying with the law, but a continuation of our respect for you and your personal information.

We undertake to preserve the confidentiality of all information you provide to us, and hope that you reciprocate.

Our policy complies with the Data Protection Act 2018 (Act) accordingly incorporating the EU General Data Protection Regulation (GDPR).

The law requires us to tell you about your rights and our obligations to you in regard to the processing and control of your personal data. We do this now, by requesting that you read the information provided at http://www.knowyourprivacyrights.org

Except as set out below, we do not share, or sell, or disclose to a third party, any information collected through our business activities.

Data Protection Officer

We have appointed a data protection officer (DPO) who is responsible for ensuring that our policy is followed.

If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact our DPO, Brian McReynolds at brian.mcreynolds@enterpriseeast.org.

Data we process

We may collect, use and store different kinds of personal data about you.
We have collated these as follows:

Your identity includes information such as first name, last name, title, date of birth, and other identifiers that you will have provided upon commencement of employment

Your contact information includes information such as delivery address, email address, telephone numbers and any other information you have given to us for the purpose of communication, service delivery, or meetings.

Your financial data includes information such as your bank account details.

Special personal information.

Special personal information is data about your race or ethnicity, religious or philosophical beliefs and information about your health.

It also includes information about criminal convictions.

We may collect special personal information about you if there is a lawful basis on which to do so.

If you do not provide personal information that we need

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform that contract. If so, we will notify you of this at the time.

If the basis changes then if required by law we shall notify you of the change and of any new basis under which we have determined that we can continue to process your information.

Context & Overview

Introduction:

What is the GDPR?

The General Data Protection Regulation (GDPR) came into force on 25 May 2018 and replaces the current Data Protection Act 1998 (DPA).

Data Protection Policy

The organisation is committed fully to compliance with the requirements of the General Data Protection Regulation (GDPR). The GDPR applies to all organisations that process data about their employees, as well as others, eg customers and clients. It sets out principles which should be followed by those who process data, and it gives rights to those whose data is being processed.

To this end, the organisation endorses and adheres fully to observing the eight individual rights set out under the GDPR, these are the following.

1. The right to be informed.
2. The right of access.
3. The right to rectification.
4. The right to erasure.
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights related to automated decision making and profiling

The bases on which we process information about you

The law requires us to determine under which of six defined bases we process different categories of your personal information, and to notify you of the basis for each category.

If a basis on which we process your personal information is no longer relevant, then we shall immediately stop processing your data.

Enterprise East 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 Data Protection act 2018 .

Why this policy exists

This data protection policy ensures Enterprise East Group CIC
- 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

The Data Protection Act 2018

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

The responsibility around using personal data has to follow strict rules called 'data protection principles' and we must ensure that the information is:

- used fairly, lawfully, and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant, and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction, or damage

People, risks and responsibilities

Policy scope
This policy applies to:
- The head office of Enterprise East

- All branches of Enterprise East
- All staff and volunteers of Enterprise East
- All contractors, suppliers and other people working on behalf of Enterprise East

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the . 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 Enterprise East 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 Enterprise East has some responsibility for ensuring data is collected, stored and handled appropriately.
Each individual or team that handles personal data must ensure that it is handled and processed in line with this policy and the data protection principles.
However, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that Enterprise East meets its legal obligations.
- The [data protection officer], Brian McReynolds, 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 Enterprise East 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.

The IT Manager, 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.
- 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 the purpose of their work.
Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
Enterprise East 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.
- 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 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 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 smart phones without password protection.
- 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 Enterprise East 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 email without password protection, 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 Data Protection Act requires Enterprise East 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 Enterprise East 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.

- Enterprise East will make it easy for data subjects to update the information Enterprise East holds 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.
- 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 Enterprise East 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 should 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 DPO at info@enterpriseeast.org. The DPO can supply a standard request form, although individuals do not have to use this.
Individuals will be charged £10 per subject access request. The DPO will aim to provide the relevant data within 14 days.
The DPO 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, Enterprise East will disclose requested data. However, the DPO will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers, if necessary.

Providing information

Enterprise East 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, a version of which is also available on the company's website, or via our HR department.