Energy Performance Nationwide – General Data Protection Regulation Policy (GDPR)

Introduction

This policy outlines how Energy Performance Nationwide collects, handles and stores personal data and ensures the law and standards surrounding data protection is respected.

Energy Performance Nationwide receives, gathers and uses certain information about individuals in the daily course of our business and this includes customers, suppliers, business contacts and other people the organisation has a relationship with or may need to contact.

Why This Policy Exists

This data protection policy has been put in place to ensure:

1. Data protection law is upheld
2. Measurable practices are in place
3. The rights of customers and partners are respected
4. Transparency exists on how individuals' data is processed and stored
5. Energy Performance Nationwide protects itself from the risks of a data breach

Data Protection Law

The General Data Protection Regulation (GDPR) takes effect on May 25, 2018 replacing the existing Data Protection Directive. It details how companies gather, 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.

GDPR ensures how personal data is gathered and managed and is underpinned by eight important principles, namely to;

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

The policy extends to and covers the following;

1. The trading office of Energy Performance Nationwide

2. All staff and volunteers of Energy Performance Nationwide

3. All contractors, suppliers and other people working on behalf of Energy Performance Nationwide

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include;

1. Names of individuals
2. Postal addresses
3. Email addresses
4. Telephone numbers
5. Any other information relating to individuals

Data Protection Risks

This policy is intended to help protect Energy Performance Nationwide from the damage of potential data security risks, including;

1. Breaches of confidentiality. *example - information being given out inappropriately*
2. *Failing to offer choice. example - all individuals should be free to choose how the company uses data relating to them*
3. Reputational damage. *example - successful access to sensitive data by hackers*

Responsibilities

Energy Performance Nationwide is responsible for ensuring data is gathered appropriately and must ensure that it is handled and processed in line with this policy and data protection principles.

David Fox is responsible for ensuring Energy Performance Nationwide meets its legal obligations. In capacity of data protection officer, David Fox is responsible for;

1. Reviewing all data protection procedures and associated policies, in line with an agreed schedule

2. Handling data protection questions covered by this policy

3. Dealing with 'subject access requests' to view the data held by Energy Performance Nationwide about the individual

4. Checking and approving contracts or agreements with third parties that may handle the company's sensitive data

General Guidelines

Data covered by this policy should be solely accessed for work purposes and should not be shared informally. Energy Performance Nationwide pledges to keep all data secure, by taking appropriate precautions and following the guidelines below;

1. Strong passwords must be used, and they should never be shared

2. Personal data should be kept strictly private and confidential and should not be disclosed to unauthorized people, either internally within the company or externally

3. Data should be regularly reviewed and updated if it is found to be out of date. If the data is no longer required, it should be deleted or removed

4. An annual audit of data will occur to ensure best practice exists

5. In the event of a data breach, the data controller must notify the appropriate authorities within 72 hours. Additionally, if the breach is likely to result in a high risk to the rights and freedoms of individuals, organizations will also need to notify affected individuals without undue delay.

Data Storage

The methods of how and where data is safely stored is outlined below.

Further questions relating to the storage of data should be directed to David Fox in his capacity of data controller.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason;

1. When not required, the paper or files should be kept in a locked drawer or filing cabinet

2. Energy Performance Nationwide endeavours to ensure papers and printouts are not left in view of unauthorised people

3. Data printouts should be shredded and disposed of securely when no longer required

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

5. Data should be protected by strong passwords that are changed regularly and never shared

6. If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not in use

7. Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service

8. Servers containing personal data should be sited in a secure location, away from general office space

9. Data should be backed up frequently and tested regularly, in line with the company's standard backup procedures

10. Data should never be saved directly to laptops or other mobile devices such as tablets or smart phones

11. All servers and computers containing data should be protected by approved security software and firewalls

Data Use

Personal data will only be used by Energy Performance Nationwide when it is justifiable and appropriate. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft;

1. When working with personal data, Energy Performance Nationwide will ensure due diligence occurs, for instance, computer screens are locked when left unattended

2. Personal data will only be shared with appropriate customers, suppliers, business contacts and other people within the course of our justifiable business relationships once appropriate consent has been granted

3. Personal data should never be transferred outside of the European Economic Area

4. Employees should not save copies of personal data to their own computers

Data Accuracy

Energy Performance Nationwide commits to taking reasonable steps to ensure data is kept accurate and up to date and the following are appropriate means of measurable checks and standards;

1. Data will be held in as few places as necessary (bespoke CRM)

2. Energy Performance Nationwide should take every opportunity to ensure data is updated where appropriate

3. Energy Performance Nationwide will make it easy for data subjects to update the information it holds about them

4. Data should be updated and/or removed from the database as and when inaccuracies are discovered

5. It is the Data Protection Officers 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 Energy Performance Nationwide are entitled to;

1. Ask what information the company holds about them and why 2. Ask how to gain access to it 3. Be informed how to keep it up to date 4. Be informed how the company is meeting its data protection obligations

In the event individuals contact Energy Performance Nationwide requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email and addressed to info@energyperformancenationwide.co.uk

1. The data controller will supply a standard request form, although individuals do not have to use this

2. The data controller will aim to provide the relevant data within 28 days

3. 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 GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances Energy Performance Nationwide will comply once satisfied the request is legitimate, seeking assistance from the company's legal advisers where necessary.

Providing Information

Energy Performance Nationwide aims to ensure that individuals are aware that their data is being processed, and that they understand;

1. How the data is being used

2. How to exercise their rights

A separate privacy statement, setting out how data relating to individuals is used by Energy Performance Nationwide is available on request.