Pro-Door Limited

Data Protection Policy
Introduction

We Are: Pro-Door Ltd
Registration Number: 3801177
Our Registered Address: Baldwin’s
5 Pullman Court
Great Western Road
Gloucester
GL1 3ND

Pro-Door Ltd 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, handles and stored to meet the company’s data protection standards – and to comply with the law.

Why this policy exists

The General Data Protection Regulation (GDPR), came into force in May 2016, but did not become enforceable until 25th May 2018.

This data protection policy ensures Pro-Door Ltd:
• Complies with the data protection law in line with GDPR 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 risk of data breach

Data protection law

The Data Protection Act 1998 describes how organisations – including Pro-Door Ltd – 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 under pinned 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

Policy Scope

This policy applies to:

- Pro-Door Ltd
- All staff
- All contractors, suppliers and other people working on behalf of Pro-Door Ltd.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside the Data Protection Act 1998. This can include:

- Names of Individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Gender
- …plus any other information relating to individuals

What Information We Collect and Why?

We may collect and store the following types of personal information:

- Information provided by yourselves when registering with us and creating an account.
- Information relating to transactions that have been made between us and yourselves, including related information to purchase of our good and services.
- Any other information that you may choose to send us.
- Communications between us and yourselves, including emails, letters and calls, when you’ve contacted us, or we’ve contact yourselves.
- Any feedback given be yourselves in reply to requests for feedback or in participating of our surveys.

The information we collect, what it is used for and the legal basis for us processing this under the General Data Protection Regulations differs, depending on your relationship with us.
Customers

<table>
<thead>
<tr>
<th>Information Collected</th>
<th>What is it Used for?</th>
<th>What is the legal base for collecting this information?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correspondence to your account (invoices, statements, payment collections etc.)</td>
<td>Maintaining and updating your account.</td>
<td>To perform a contract and to maintain your account.</td>
</tr>
<tr>
<td>Your account details management purposes (Company name, contact, email, address etc.)</td>
<td>Maintaining your account and providing you with goods and services upon your request.</td>
<td>To perform a contract and to maintain your account.</td>
</tr>
<tr>
<td>Any posts or messages made by yourself on social media that is directed to us.</td>
<td>Communicating with a response to your questions or comments.</td>
<td>To answer your comments or queries.</td>
</tr>
</tbody>
</table>

Prospective Customers

<table>
<thead>
<tr>
<th>Information Collected</th>
<th>What is it Used for?</th>
<th>What is the legal base for collecting this information?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submitted Contact Details, received on signed company account forms</td>
<td>To create your account.</td>
<td>It is in the legitimate interest of a person or company that we can contact them to provide information in response to their enquiry.</td>
</tr>
<tr>
<td>Any posts or messages made by yourself on social media that is directed to us.</td>
<td>Communicating with a response to your questions or comments.</td>
<td>To answer your comments or queries.</td>
</tr>
<tr>
<td>Names, Addresses, telephone numbers and email addresses may be required when answering a quotation request.</td>
<td>We will use the information provided to submit our quotation to yourselves</td>
<td>To enable us to provide you with a quote upon request.</td>
</tr>
<tr>
<td>Prior to opening an account, we may use your name/company name to run a credit report using third party software</td>
<td>To obtain a credit score to decide whether to proceed with an account.</td>
<td>It is in the legitimate interest of the company to establish whether we are able to offer you credit terms.</td>
</tr>
</tbody>
</table>
Suppliers

<table>
<thead>
<tr>
<th>Information Collected</th>
<th>What is it Used for?</th>
<th>What is the legal base for collecting this information?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any posts or messages made by yourself on social media that is directed to us.</td>
<td>Communicating with a response to your questions or comments.</td>
<td>To answer your comments or queries.</td>
</tr>
<tr>
<td>Contact Names, Bank Details, Email Address and Postal Address.</td>
<td>To enable us to manage and maintain your account and create a transaction.</td>
<td>This is a legitimate interest to allow us to create a contract and make payments.</td>
</tr>
</tbody>
</table>

Employees

<table>
<thead>
<tr>
<th>Information Collected</th>
<th>What is it Used for?</th>
<th>What is the legal base for collecting this information?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal and Confidential information that relates to employment and well-being.</td>
<td>To allow us to legally comply and administer to UK government legislation</td>
<td>In order to comply with UK government law and perform a contract.</td>
</tr>
<tr>
<td>Banking and Tax Details</td>
<td>To provide to our accountants to pay employees via payroll activities and comply with HMRC.</td>
<td>To enable us to pay our employee in compliance with HMRC.</td>
</tr>
</tbody>
</table>

Data Protection Risks

This policy helps to protect Pro-Door Ltd 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 Pro-Door Ltd 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 the policy and data principles.
However, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that Pro-Door Ltd meets its legal obligations.
- Pro-Door Ltd’s Data Controller is Linda Jenkins – Managing Director.
- The Data Protection Officer, Gemma Jones, 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 Pro-Door Ltd 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, Linda Jenkins, 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.

**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.
- Pro-Door Ltd 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 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.
- Pro-Door Ltd’s standard policy is all information and documents are kept filed for 6 years, in line with the company accounts procedure. HMRC legal obligations – we are required to keep records (invoices and contracts) for 6 years from the end of the latest financial year.
Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Monitoring

Do not record phone calls. We have a CCTV system in place in our office for security measures. These are recorded for one month.

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 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 firewall.
Data use

Personal Data is of no value to Pro-Door Ltd 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, 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 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 Pro-Door Ltd 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 Pro-Door Ltd 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 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.
- Pro-Door Ltd will make it easy for data subjects to update the information Pro-Door Ltd holds about them.
- 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.

Data breach reporting

New requirements under GDPR specify that data breaches involving personal data are reported the Information Commissioner’s Office within 72 hours of becoming aware of the breach. This is unless Pro-Door Ltd is able to prove that a personal data breach has little to no risk of impacting on an individual’s rights. In the case of a breach Pro-Door Ltd will review current incident management processes to ensure that breach reporting (to either a supervisory authority or the data subjects themselves) is addressed and the requirements accessed at the point the incident is identified.
Subjects access requests

All individuals who are the subject pf personal data by Pro-Door Ltd 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.

Subjects access requests from individuals should be made by Email, addressed to the data controller at info@pro-door.co.uk. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10.00 per subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making the subject access request before handling over any information.

**Disclosing data for other reasons**

Pro-Door Ltd do not pass on any personal data to third parties for marketing purposes.

Pro-Door may use your name/company name and address to run a credit check using third party software prior to opening a 30 days credit account.

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

Under these circumstances, Pro-Door Ltd 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**

Pro-Door aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How data is being used
- How to exercise their rights

To these ends, the company has a privacy notice for employees, setting out how data relating to individuals is used by the company.