

GDPR Compliant Privacy Policy

Context and Overview

Key Details

Introduction:

Kent Flush Doors & Joinery Ltd needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people, Kent Flush Doors & Joinery Ltd has a relationship with or may need to contact.

This policy describes how 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 Kent Flush Doors & Joinery Ltd

- 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 risk of a data breach

Data Protection Law

The Data Protection Act 1998 describes how organisations including Kent Flush Doors & Joinery 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 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 to be held 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 Kent Flush Doors & Joinery Ltd
- All employees of Kent Flush Doors & Joinery Ltd
- All contractors, suppliers and other persons working on behalf of Kent Flush Doors & Joinery 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
- Plus any other information relating to individuals

Data Protection Risks

This policy helps to protect Kent Flush Doors & Joinery 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 gained access to sensitive data.

Responsibilities

Everyone who works for or with Kent Flush Doors & Joinery Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person 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 Management Team** is ultimately responsible for ensuring that Kent Flush Doors & Joinery Ltd meets its legal obligations
- **The Data Protection Representative** is responsible for:
 - Keeping the Management Team 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 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 Kent Flush Doors & Joinery 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 Managing Director** 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 correctly
 - Evaluating any third party services the company is considering using to store, or process data. For instance cloud computing services
- **The Managing Director** is responsible for
 - Approving any data protection statements attached to communications such as emails and letters
 - Addressing any data protection queries from journalists or media outlets such as newspapers
 - Where necessary working with other staff to ensure marketing initiatives abide by data protection principles

General Staff Guidelines

- The only persons able to access data covered by this policy should be those who need it for their day to day work activity
- Data should not be shared informally. When access to confidential information is required, employees can request it through their immediate line manager
- Kent Flush Doors & Joinery 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 the guidelines below
- Strong passwords must be used and they never should be shared
- Personal data should not be disclosed to unauthorised persons, 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 assistance from their immediate line manager or the data protection representative if they are unsure about any aspect of data protection

Data Storage

These rules describe how and where data should be safely stored. Questions regarding the safe storage of data should be directed to the Managing Director

Where data is stored in manuscript form, it should be kept in a secure place where unauthorised persons 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 manuscript files should be maintained in secure lockable storage
- Employees should ensure that manuscript documents, printouts etc are not left where unauthorised persons could see them
- 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, it should be locked away when not use
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service
- Data should be backed up frequently. Those backups should be tested regularly in line with company 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 Kent Flush Doors & Joinery 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 to 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 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 Kent Flush Doors & Joinery Ltd to take reasonable steps to ensure data is kept accurate and up to date

The more important is that the personal data is accurate, the greater the effort Kent Flush Doors & Joinery Ltd should put into ensuring its accuracy.

- 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 details when they call
- 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 Managing Director'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 Kent Flush Doors & Joinery Ltd are entitled to

- Ask what information, the company holds on them and why
- Ask how to gain access to it
- Be informed of how to keep it up to date
- Be informed on 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

Subject access requests from individuals should be made by email addressed to the company's email address

The company will always verify the identity of anyone making a subject access request before releasing 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, Kent Flush Doors & Joinery Ltd will disclose requested data. However the data provider will ensure the request is legitimate, seeking assistance from the Management Team and from the company's legal advisers where necessary.

Providing Information

Kent Flush Doors & Joinery Ltd 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, 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 web site