



## **Data Protection Policy**

Policy prepared by: Darren Ayres  
Operational date: 20<sup>th</sup> May 2018  
Review date: 20<sup>th</sup> May 2020

### **Introduction**

JMDA Limited needs to gather and use certain information about individuals. These can include customers, suppliers, business contracts, sub-contractors, employees and other people the company 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 that JMDA Limited:

- Complies with the General Data Protection Regulation (GDPR) and follows good practice.
- Protects the rights of staff, customers and partners.
- Is open about how it stores and processes' individual's data.
- Protects itself from the risks of a data breach.

### **Data protection principles**

Data protection is centred around several key principles and Article 5 of the General Data Protection Regulation (GDPR) stipulates that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;



e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

**In summary, only required personal data should be held, it must be secured and protected against loss, and only kept as long as is necessary.**

### **Policy Scope**

This policy applies to:

- All employees of JMDA Limited.
- All sub-contractors, suppliers and other people working on behalf of JMDA Limited.

It applies to all data the company holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation (GDPR). This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

### **Data Protection Risks**

This policy helps to protect JMDA Limited from data security risks, including:

- **Breaches of confidentiality** i.e. information being given out inappropriately.
- **Failing to offer choice** i.e. all individuals should be given a choice as to how a company uses data relating to them.
- **Reputational damage** i.e. JMDA Limited could suffer if hackers successfully gained access to sensitive data.

### **Responsibilities**

Everybody who works for or with JMDA Limited has some responsibility for ensuring data is collected, stored and handled appropriately.

All individuals that handle personal data must ensure they it is handled and processed in line with this Data Protection Policy.



However, the Directors have ultimate responsibility for ensuring that JMDA Limited meets its legal obligations:

- Reviewing the Data Protection Policy and updating the content (as necessary) every two (2) years.
- Ensuring all staff and relevant persons read a copy of the Data Protection Policy and are fully aware of the content. For this purpose, a copy is available via JMDA's website; [www.jmdainteriors.co.uk](http://www.jmdainteriors.co.uk)
- Handling Data Protection questions which result from receipt of this policy.
- Dealing with requests from individuals to see the data JMDA Limited 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.
- 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 i.e. cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.

### **General Guidelines**

- The only people able to access data covered by this policy should be those that need it for their work.
- Data should not be shared informally.
- JMDA Limited will ensure a copy of their Data Protection Policy is available to read for all employees, sub-contractors and other relevant people to help them understand their responsibilities when handling data on behalf of JMDA Limited.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below:
  - Strong passwords must be used and they must never be shared
  - Personal data must 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 it is found to be no longer required it should be deleted and disposed of securely.

### **Data Storage**

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 which is usually stored electronically, but had been printed out onto paper.

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



- Employees should make sure paper copies are not left in an area where unauthorised people may see them i.e. on a printer.
- Data print outs should be securely shredded and disposed of 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 i.e. USB devices or CDs, these should be locked securely when not in use.
- Data should only be stored on designated drives and should only be uploaded to approved cloud computing services.
- Data should be backed up frequently.
- Data should never be saved directly to laptops or mobile devices like tablets or smart phones.
- All computers should be protected by appropriate security software and a firewall.

### **Data Use**

Personal data is of no use to JMDA Limited unless the business can make use of it. However, it is when personal data is accessed and used that it can be of the greatest risk of loss, corruption or theft.

- When working with personal data, employees should lock their computer screens when left unattended.
- Personal data should not be shared informally.
- Personal data should not be transferred outside of the European Economic Area (EEA).
- 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 JMDA Limited to take reasonable steps to ensure data is kept accurate and up to date:

- Data will be held in as a few places as possible. Duplicate copies should be avoided.
- Employees should take every opportunity to ensure data is updated i.e. confirming a customer's details when they call.
- Data should be updated as inaccuracies become apparent i.e. if a contacts telephone changes or a customer moves.

### **Subject Access Requests**

All individuals who are the subject of personal data held by JMDA Limited 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 JMDA Limited to request this information, this is called a 'Subject Access Request'.

Subject Access Requests should be made via email, addressed to the Directors at the registered office address.

The Director will always verify the identity of any Subject Access Requests before sharing any information.