Data Protection Policy – Edge Building Products Ltd

Policy information	
Organisation	Edge Building Products Ltd
Scope of policy	This policy covers all branches of Edge Building Products Ltd, all of which are located in the United Kingdom
Policy operational date	4th May 2018
Policy prepared by	Kieran Napthine
Date approved by Board/ Management Committee	4th May 2018
Policy review date	3rd May 2021

Introduction	
Purpose of policy	Our reasons for processing data are as follows: • complying with the law • following good practice • protecting clients, staff and other individuals • protecting the organisation
Types of data	We collect data on customers (contact information, purchase history, history of contact with members of our organisation), Suppliers (contact information, purchase history, history of contact with members of our organisation), Employees (contact information, ethnicity, gender, health, driving licence, training and other accreditation, history of contact with members of our organisation),
Policy statement	We commit to: • comply with both the law and good practice • respect individuals' rights • be open and honest with individuals whose data is held • provide training and support for staff who handle personal data, so that they can act confidently and consistently • Notify the Information Commissioner voluntarily, even if this is not required
Key risks	The main risks with in our organisation are: • information about data getting into the wrong hands, through poor security or inappropriate disclosure of information • individuals being harmed through data being inaccurate or insufficient

Responsibilities	
Company Directors	JD Napthine, EM Napthine, KD Napthine, SE Napthine
Data Protection Officer	Kieran Napthine Responsibilities include: • Briefing the Board on Data Protection responsibilities • Reviewing Data Protection and related policies • Advising other staff on tricky Data Protection issues • Ensuring that Data Protection induction and training takes place • Notification to the ICO • Handling subject access requests • Approving unusual or controversial disclosures of personal data • Approving contracts with Data Processors
Specific Department Heads	n/a
Employees & Volunteers	All staff and volunteers are be required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. (From now on, where 'employees' is used, this includes both paid employees and volunteers.)
Enforcement	We provide training on the requirements of GDPR for data processing. Infringement of this data protection policy carries penalties.

Security	
Security measures	All databases are password protected. Customer & supplier information access is controlled via the permission based system within the companies ERP software. Employee information is handled via a secure cloud based system with access only granted to directors and managers.
Business continuity	Data is backed up securely on the cloud.
Specific risks	When data is being worked on outside of the business premises, eg. where an employee has permission to access this from home or at a customer's premises then additional care should be taken that no data is exposed to persons outside of the organisation or within the organisation that do not need to access the data. Employees are advised to be particularly careful when opening emails. If an email comes from an unknown contact, or from a known contact but with unusual content, please be extremely careful when opening it, do not open it if you have any reservations as to the content and contact the sender by another means (eg phone) to confirm validity. When data is received over the phone, data processors must ensure that this data is entered into the relevant secure database as soon as possible and any hard copy notes of the data are securely destroyed, eg. By shredding.

Data recording and storage	
Accuracy	We make every effort to ensure data is accurate, when details are given verbally, ie over the phone, we recommend that data processors check the information against information made available on the supplier/customers website where possible. If any inaccuracy is identified, we ask that all employees are vigilant in informing the relevant data processor so that corrections can be made.
Updating	We ask that all employees are vigilant in informing the relevant data processor so that corrections can be made.
Storage	Electronic information should only be stored on the servers of PCs belonging to the company or on storage drives belonging to the company. Hard copy information must not leave the premises of the company.
Retention periods	Most data is kept for a minimum of 7 years in order to comply with taxation laws, after 7 years data may be destroyed
Archiving	When archived data is destroyed, we permanently delete it from our IT systems, any hard copy data is shredded on a periodic basis.

Right of Access	
Responsibility	The data protection officer is responsible for ensuring that right of access requests are handled within the legal time limit of one month
Procedure for making request	Right of access requests must be in writing to a current branch address operated by the business. They must be address to the Data Protection Officer or Directors of the company. Employees are responsible to ensure that anything which might be subject to an access request is passed to the Data Protection officer without delay.
Provision for verifying identity	Where the person requesting access is not known personally to the Data Protection Officer, we will ask to see at least 2 items of personal ID before granting access. Eg Passport, driving licence.
Charging	The company will provide the information free of charge apart from when a request is manifestly unfounded or excessive, particularly if it is repetitive, where a fee of £20 + VAT will be charged. Further requests for copies of the above information will be charge at £10/copy + VAT.
Procedure for granting access	If the request is made electronically, we will provide the information in a commonly used electronic format such as PDF. For users of our web-portal, much of the information we hold is visible to them online and can be updated by the customer directly.

Transparency	
Commitment	The organisation is committed to ensuring that Data Subjects are aware that their data is being processed and • for what purpose it is being processed • what types of disclosure are likely, and • how to exercise their rights in relation to the data
Procedure	Standard ways for Data Subjects to be informed include: • the handbook for employees • during the initial interview with clients • on the web site
Responsibility	All staff, under the supervision of the Data Protection Officer

Lawful Basis	
Underlying principles	The lawful basis of recording the data we hold are as below: • Consent – we obtain consent for e-marketing purposes, consent is stored within Mail Chimp system • Legal Obligation – we hold customer & supplier records to comply with tax accounting laws • Contract – we hold customer, supplier and employee records because we have a contract with them.
Opting out	People are given the option to opt out of our marketing database at anytime via an online form
Withdrawing consent	The organisation acknowledges that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where the organisation has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn

Employee training & Acceptance of responsibilities	
Induction	All employees who have access to any kind of personal data will have their responsibilities outlined during their induction procedures
Continuing training	The company will endeavour to remind staff of Data Protection issues periodically as part of their ongoing training
Procedure for staff signifying acceptance of policy	The policy will be circulated and employees are required to e-sign that they have received and understood the policy and agree to comply with it.

Policy review	
Responsibility	Data Protection Officer
Procedure	Key staff in customer service, HR & purchasing may be consulted during the review procedure to ensure compliance throughout the organisation.
Timing	The review should be started at least 1 week before the review date to ensure completion by the review date.