General Data Protection Regulation of OKD Ltd 2018

I. Context and overview key details

- Policy prepared by: Leigh Warriner

- Company Name: Outdoor Kitchens & Design Ltd

- Company Address: OKD, Units E & F, The Old Brickyard, Ashton Keynes, SN6 6QR.

II. Introduction

Outdoor Kitchens & Design Ltd need to gather and use certain information about individuals in the course of conducting their business.

These can include customers, suppliers, business contacts, employees and other people the business 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.

III. Why this policy exists

This General Data Protection Regulation 2018 Policy ensures that OKD:

• Follows good practice and complies with the data protection law

• Protects the rights of staff, customers and partners

• Is open about how it stores and processes individuals data

• Protects itself from the risks of a data breach

IV. General Data Protection Regulation 2018

The General Data Protection Regulation 2018 describes how organisations — including OKD — 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 General Data Protection Regulation 2018 is underpinned by six important principles. These say that personal data must be:

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

2) 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 incompatible with the initial purposes;

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

4) 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;

5) 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;

6) 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.

V. Data protection risks

This policy helps to protect OKD 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.

VI. People, risks and responsibilities policy scope

This policy applies to:

• The OKD office

• All staff of OKD

• All contractors, suppliers and others working on behalf of OKD

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation 2018. This can include:

• Names of individuals

• Postal addresses

• Email addresses

• Telephone numbers

• Plus any other information relating to individuals

VII. Responsibilities

Everyone who works for or with OKD has some responsibility for ensuring data is collected, stored and handled appropriately.

Each individual that handles personal data must ensure that it is handled and processed in line with this policy and General Data Protection Regulation 2018 principles.

However, these people have key areas of responsibility:

• The Board of Directors is ultimately responsible for ensuring that OKD meets its legal obligations and is responsible for:

o Reviewing all data protection procedures and related policies, in line with an agreed schedule.

o Arranging data protection training and advice for the people covered by this policy.

o Handling data protection questions from staff and anyone else covered by this policy.

o Dealing with requests from individuals to see the data OKD holds about them (also called 'subject access requests').

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

o Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

o Performing regular checks and scans to ensure security hardware and software is functioning properly.

o Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

o Approving any data protection statements attached to communications such as emails and letters.

o Addressing any data protection queries from journalists or media outlets like newspapers.

o Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

VIII. 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.

• Employees should keep all data secure, by taking sensible precautions and following the 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.

IX. Providing Information

OKD 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.

X. Disclosing data for other reasons

In certain circumstances, the General Data Protection Regulation 2018 allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, OKD will disclose the requested data. However, the Directors will ensure the request is legitimate before passing on any information.

XI. Security

We constantly review the encryption methods and levels of our digital files that are required to be transferred. We use security software to test our network for vulnerabilities. Data is stored on a closed network with no outside connection to prevent cyber attacks.

All individuals who are the subject of personal data held by OKD 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.

• How OKD remove the personal data

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 Leigh Warriner at info@okdltd.com. We will always verify the identity of anyone making a subject access request before handing over any information.

XII. Payments

Any visa, credit card and cheque payments are processed in a secure office with key pad entry system which only authorised employees have access to. Visa and credit card slips are then stored securely for a period of three months when they are securely destroyed.

XIII. Online Ordering

Card payments are provided by Square who deal with the complete process of handling the card payments. This means that we do not process payment information and do not store it ourselves. The payment is transacted through Secure Server Software, which encrypts all the information so that it can't be intercepted.

Orders that are sent to home addresses are not sent with any identifiable data other than name and address of the person who placed the order.

XIV. Data Retention

OKD collects and uses personal data to administer orders and deliver goods. We also use it to anticipate and resolve queries.

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to Leigh Warriner (Director). We do not disclose this data to any third parties.

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 are kept in a locked drawer or filing cabinet.
- Employees make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts are 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 is protected by strong passwords that are changed regularly and never shared between employees.
- Data is backed up frequently. Those backups are tested regularly, in line with the company's standard backup procedures.
- All servers and computers containing data are protected by approved security software and a firewall.

Personal data is of no value to OKD 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:

- Personal data is not shared informally.
- Personal data should never be transferred outside of the European Economic Area.

The law requires OKD 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 OKD should put into ensuring its accuracy.

SIGNED.....L.G.Warriner.....

NAME LEIGH GEORGETTE WARRINER (DIRECTOR)

DATE.....22/5/18.....