CREAGH

GDPR POLICY

Rev 2 Jan 2022

INTRODUCTION

On 25th May 2018, the General Data Protection Regulations (GDPR) were enforced across Europe, including the UK. The Law aims to give citizens more control over their data and affects businesses which hold personal data on customers, prospects or employees. The definition of personal data covers anything that points to someone's professional or personal life including (but not limited to) names, photographs, emails addresses, IDs, bank details, phone numbers, medical information and computer IP addresses.

Creagh Concrete Products Limited ('the Company') stands committed to the development of secure policies and practices and respecting the rights and privacy of all employees, sub-contractors, customers, suppliers and any other third parties associated with the Company, in accordance with the General Data Protection Regulation (GDPR) May 2018.

The GDPR contains provisions that the Company is aware of as data controllers, including provisions intended to enhance the protection of employee's personal data.

COMPLIANCE

This policy applies to all employees of the Company. Any breach of this policy or of the Regulation itself will be considered an offence and the Company's disciplinary procedures will be invoked.

As a matter of best practice, sub- contractors and suppliers working with the Company who have access to personal information, will be expected to read and comply with this policy also. This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

RESPONSIBILITIES UNDER THE GDPR

The Company will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data. The Company has a Data Protection Manager, currently the HR Director who is available to address any concerns regarding the data held by the Company and how it is processed, held and used.

DATA PROTECTION PRINCIPLES

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles.

1. PROCESS PERSONAL DATA FAIRLY AND LAWFULLY.

The Company will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

2. PROCESS THE DATA FOR THE SPECIFIC AND LAWFUL PURPOSE FOR WHICH IT COLLECTED THAT DATA AND NOT FURTHER PROCESS THE DATA IN A MANNER INCOMPATIBLE WITH THIS PURPOSE.

The Company will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3. ENSURE THAT THE DATA IS ADEQUATE, RELEVANT AND NOT EXCESSIVE IN RELATION TO THE PURPOSE FOR WHICH IT IS PROCESSED.

The Company will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained.

4. KEEP PERSONAL DATA ACCURATE AND, WHERE NECESSARY, UP TO DATE.

The Company will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the Company if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the Company to ensure that any notification regarding the change is noted and acted on.

5. ONLY KEEP PERSONAL DATA FOR AS LONG AS IS NECESSARY.

The Company undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. The Company will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste).

6. PROCESS PERSONAL DATA IN ACCORDANCE WITH THE RIGHTS OF THE DATA SUBJECT UNDER THE LEGISLATION.

Individuals have various rights under the legislation including a right to:

- Be told the nature of the information the Company holds and any parties to whom this may be disclosed.
- Prevent processing likely to cause damage or distress.
- Prevent processing for purposes of direct marketing.
- Sue for compensation if they suffer damage by any contravention of the legislation.
- Take action to rectify, block, erase or destroy inaccurate data.
- Request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

The Company will only process personal data in accordance with individuals' rights.

7. PUT APPROPRIATE TECHNICAL AND ORGANISATIONAL MEASURES IN PLACE AGAINST UNAUTHORISED OR UNLAWFUL PROCESSING OF PERSONAL DATA, AND AGAINST ACCIDENTAL LOSS OR DESTRUCTION OF DATA.

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties. The Company will ensure that all personal data is accessible only to those who have a valid reason for using it. The Company has in place appropriate security measures e.g. ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):

- Keeping all personal data in a lockable cabinet with key-controlled access.
- Password protecting personal data held electronically.
- Archiving personal data which are then kept securely (lockable cabinet).
- Placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff.
- Ensuring that PC screens are autolocked if left unattended

In addition, the Company has in place appropriate measures for the deletion of personal data - manual records will be shredded or disposed of as 'confidential waste'. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically.

This policy also applies to staff and students who process personal data 'off-site', e.g. when working at home, and in circumstances additional care must be taken regarding the security of the data.

8. ENSURE THAT NO PERSONAL DATA IS TRANSFERRED TO A COUNTRY OR A TERRITORY OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA) UNLESS THAT COUNTRY OR TERRITORY ENSURES ADEQUATE LEVEL OF PROTECTION FOR THE RIGHTS AND FREEDOMS OF DATA SUBJECTS IN RELATION TO THE PROCESSING OF PERSONAL DATA.

The Company will not transfer data to such territories without the explicit consent of the individual.

When the Company collects personal data in any form via its website, it has a clear and detailed privacy statement on the website.

SUBJECT ACCESS RIGHTS (SARS)

Individuals have a right to access personal data relating to them which is held by the Company. Any individual wishing to exercise this right should apply in writing to the Data Protection Manager. Any employee receiving a SAR should forward this to the Data Protection Manager. See Company SAR Policy.

CCTV

There are some CCTV systems operating within the Company for the purpose of protecting employees and property. The Company will only process personal data obtained by the CCTV system in a manner which ensures compliance with the legislation. See Company CCTV Policy.

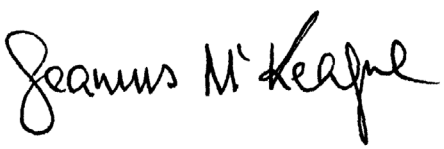
COMPANY POLICIES WHICH IMPLEMENT GDPR

The Company has implemented the following Policies to ensure compliance with GDPR:-

- Clean Desk and Disposal of Confidential Waste Policy; this Policy is directed at employees to ensure that no personal data is left unsecured within the office environment and that all data is responsibly disposed of.
- Breach Management Plan; explains the Company's procedures and protocols should a data breach occur.
- CCTV Policy: explains how and why we record CCTV images within each of our locations.
- SAR (Subject Access Request) Policy: explains how requests can be made to the Company for access to what data we hold on that individual.
- Employee Privacy Notice: explains to employees what data we hold on them; the duration we hold it for, who has access to same and the reasons why.
- Recruitment Privacy Notice: explains to potential candidates what information we store and retain from them via their application form or CV; the reasons why and the duration we hold same for.
- We have a Privacy Notice displayed on our Company website which explains to those who visit our website our commitment to privacy and an explanation as to what data we hold on those visiting our website or sign up to our mailing list together with information as to how to be removed from same.
- Data Retention Policy in place which sets out how long we hold each type of document and the reason
- HR Retention Policy which sets out the duration we hold each item of HR information and the reasons why.

PROCEDURE FOR REVIEW

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998.
For further information on any matter contained herein contact the Data Protection Manager; Lorna McMullan.



Chairman
Creagh Concrete Products Ltd
REV 2 – January 2022