GDPR Policy

Armstrong Group (Scotland) Ltd ("AGSL"), its subsidiaries and affiliates (Molplant Construction Ltd, Armstrong Waste Management Ltd, Armstrong Properties (Scotland) Ltd, Armstrong Renewables (Scotland) Ltd), are committed to protecting and respecting your privacy. This policy (together with our terms of use and any other documents referred to in it) sets out how we collect, use, and protect your personal information, and your rights in relation to that information. AGSL processes personal data in accordance with the data protection laws that are applicable within the United Kingdom. For any queries relating to data protection, please write to Group Managing Director, Armstrong Group, Armstrong Group Administration Office, Downsway Industrial Estate, Dumfries, DG1 3RS, or telephone on 01387-253030.

CONTENTS

Document: AG-POL-024 Version: REV 1 Date: 26.06.19	**GDPR Policy**	

1. Introduction
The GDPR came into effect in the United Kingdom on 25 May 2018. The GDPR introduced several new obligations on Data Controllers and data processors and new rights for Data Subjects.

2. Purpose
AGSL is committed to being transparent about how we collect and use the Personal Data of our customers and suppliers, members of the public and Employees, and to meeting our data protection obligations pursuant to the GDPR. This policy sets out AGSL's commitment to data protection and Data Subject rights in relation to Personal Data.

3. Scope and Effective Date
This policy applies to all companies in the Armstrong Group of companies. The effective date of this policy is 25 May 2018.

4. The Person with responsibility for Data Protection
The Group Managing Director of AGSL is the person with primary responsibility for data protection compliance within the Armstrong group of companies. If you would like to contact us with any queries or comments regarding this policy please write to Group Managing Director, Armstrong Group, Armstrong Group Administration Office, Downsway Industrial Estate, Heathhall, Dumfries, DG1 3RS or telephone 01387-253030.

5. Policy

5.1 Definition of Terms
The terms used in this policy are explained below: - “Armstrong Group of companies” or “AGSL” means all companies of which AGSL is the ultimate parent company.

“Data Controller” means the Armstrong Group Entity which determines the purposes for which and the manner in which any Personal Data is, or is to be, processed.

“Data Subject” means the individual to which the Personal Data refers.

“Employee” means any job applicant or candidate, full or part time; temporary or permanent employee, worker, contractor and former employee of any Armstrong Group company

“GDPR” means the General Data Protection Regulation (EU) 2016/679.

"Personal Data" is any information that relates to a living individual who can be identified from that information.

“Processing” is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

5.2 Data protection principles
AGSL processes Personal Data in accordance with the GDPR and the following data protection principles:

1. AGSL processes Personal Data lawfully, fairly and in a transparent manner;

2. AGSL collects Personal Data only for specified, explicit and legitimate purposes;

3. AGSL processes Personal Data only where it is adequate, relevant and limited to what is necessary for the purposes of processing;

4. AGSL keeps accurate Personal Data and takes all reasonable steps to ensure that inaccurate Personal Data is rectified or deleted without delay;

5. AGSL keeps Personal Data only for the period necessary for processing;

6. AGSL adopts appropriate measures to make sure that Personal Data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

5.2.1 Privacy Notices and Privacy Statement

AGSL tells Data Subjects the reasons for processing their Personal Data, how it uses such data and the legal basis for processing in its privacy notices

AGSL will not process Personal Data of Data Subjects for other reasons. Where AGSL relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of Data Subjects.

AGSL will update Personal Data promptly if a Data Subject advises that his/her information has changed or is inaccurate.

AGSL keeps a record of its processing activities in respect of Personal Data in accordance with the requirements of the GDPR.

5.3 Individual rights

Data Subjects have a number of rights in relation to their Personal Data.

5.3.1 Subject Access Requests

Data Subjects have the right to make a Subject Access Request ("SAR"). If an individual makes a SAR, AGSL will tell him/her:

1. whether or not his/her data is processed and if so why, the categories of Personal Data concerned and the source of the data if it is not collected from the individual;

2. to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;

3. for how long his/her Personal Data is stored (or how that period is decided);

4. his/her rights to rectification or erasure of Personal Data, or to restrict or object to processing;

5. his/her right to complain to the Information Commissioner if he/she thinks AGSL has failed to comply with his/her data protection rights;

6. whether or not AGSL carries out automated decision-making and the logic involved in any such decision-making, AGSL will also provide the individual with a copy of the Personal Data undergoing processing unless there is some lawful basis for not doing so, in which case it will inform the Data Subject of the reasons for this.

Any data provided will normally be in electronic form if the Data Subject has made a request electronically, unless he/she agrees otherwise, or it is otherwise not technically possible or practicable for AGSL to provide it electronically. To make a SAR, the Data Subject should send a letter to The Group Managing Director, Armstrong Group, Armstrong Group Administration Office, Downsway Industrial Estate, Heathhall, Dumfries, DG1 3RS

In some cases, AGSL may need to ask for proof of identification before the request can be processed. We will inform the individual if we need to verify his/her identity and the documents it requires. AGSL will normally seek to respond to a request within one month from the date it is received.

If a Data Subject submits a request that is unfounded or excessive, AGSL will notify him/her that this is the case.

5.3.2 Other rights

Data Subjects have a number of other rights in relation to their Personal Data.

They can require a Data Controller to:

1. rectify inaccurate data;

2. stop processing or erase data that is no longer necessary for the purposes of processing;

3. stop processing or erase data if the Data Subject's interests override the AGSL's legitimate grounds for processing data

4. stop processing or erase data if processing is unlawful;

5. stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the Data Subject's interests override AGSL's legitimate grounds for processing data.

To ask AGSL to take any of these steps, the Data Subject should send a SAR request to AGSL in the noted manner.

5.4 Data security

AGSL takes the security of Personal Data seriously and has internal policies and controls in place to protect Personal Data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by Employees in the proper performance of their duties.

AGSL requires all of its Employees to follow its data security measures. Where AGSL engages third parties to process Personal Data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

5.5 Privacy Impact

AGSL will consider the purposes for which activities are carried out, the risks for Data Subjects and the measures that can be put in place to mitigate those risks.

5.6 Data breaches

If AGSL discovers that there has been a breach of Personal Data that poses a risk to the rights and freedoms of Data Subjects, it will report it to the Information Commissioner. AGSL will record all data breaches regardless of their effect. If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

If Employees suspect or become aware of a data security breach, they are required to advise the Group Managing Director to enable AGSL to respond appropriately.

5.7 Individual responsibilities

Data Subjects are responsible for helping AGSL keep their Personal Data up to date. Data Subjects should let AGSL know if data provided changes.

AGSL's Employees may have access to the Personal Data of our customers, suppliers and members of the public in the course of their employment. Where this is the case, AGSL relies on its Employees to meet its data protection obligations to those customers, suppliers and members of the public.

Employees who have access to Personal Data are required:

1. to access only data that they have authority to access and only for authorised purposes;

2. not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;

3. to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

4. not to remove Personal Data, or devices containing or that can be used to access Personal Data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;

5. not to store Personal Data on local drives or on personal devices that are used for work purposes;

6. to report data breaches of which they become aware to the Group Managing Director

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under AGSL's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee, customer, supplier data or data connected with members of the public without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

5.8 Training

AGSL will provide appropriate training to relevant Employees about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Employees whose roles require regular access to Personal Data, or who are responsible for implementing this policy or responding to SARs under this policy, will receive additional training to help them understand their duties and how to comply with them.

6. Review of this Policy

AGSL will review this policy periodically and will make any required updates.

7. Further Information and Support

In the event of further queries about this policy please send a letter to The Group Managing Director, Armstrong Group, Armstrong Group Administration Office, Downsway Industrial Estate, Heathhall, Dumfries, DG1 3RS

Review

This document is reviewed annually by the Board of the Armstrong Group (Scotland) Limited on **July 2020**