



## **DATA PROTECTION POLICY**

### **External**

This policy gives important information about:

- the data protection principles with which the Company must comply;
- what is meant by personal information (or data) and sensitive personal information (or data);
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g. about the personal information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- your rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

## **1 Data protection principles**

1.1 The Company will comply with the following data protection principles when processing personal information:

- 1.1.1 we will process personal information lawfully, fairly and in a transparent manner;
- 1.1.2 we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
- 1.1.3 we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;
- 1.1.4 we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay;
- 1.1.5 we will keep personal information in a form which permits identification of data subjects for no longer than is necessary or for the purposes for which the information is processed; and

- 1.1.6 we will take appropriate technical and organisational measures to ensure that personal information are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

## **2 Basis for processing personal information**

- 2.1 In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:
  - 2.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:
    - (a) that the data subject has consented to the processing;
    - (b) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
    - (c) that the processing is necessary for compliance with a legal obligation to which the Company is subject;
    - (d) that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or
    - (e) that the processing is necessary for the purposes of legitimate interests of the Company or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject—see clause 2.2 below.
  - 2.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (ie that there is no other reasonable way to achieve that purpose);
  - 2.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
  - 2.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);
  - 2.1.5 where sensitive personal information is processed, also identify a lawful special condition for processing that information; and
  - 2.1.6 where criminal offence information is processed, also identify a lawful condition for processing that information.
- 2.2 When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing, we will:
  - 2.2.1 conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;
  - 2.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);
  - 2.2.3 keep the LIA under review, and repeat it if circumstances change; and
  - 2.2.4 include information about our legitimate interests in our relevant privacy notice(s).

## **3 Documentation and records**

- 3.1 We will keep written and electronic records of processing activities which are high risk, including:
  - 3.1.1 the name and details of the organisation;
  - 3.1.2 the purposes of the processing;

- 3.1.3 a description of the categories of individuals and categories of personal data;
  - 3.1.4 categories of recipients of personal data;
  - 3.1.5 where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;
  - 3.1.6 where possible, retention schedules; and
  - 3.1.7 where possible, a description of technical and organisational security measures.
- 3.2 You (in common with other data subjects) have the following rights in relation to your personal information:
- 3.2.1 to be informed about how, why and on what basis that information is processed;
  - 3.2.2 to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request to your line manager. to have data corrected if it is inaccurate or incomplete;
  - 3.2.3 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten')

If you wish to exercise any of the above please send an e-mail to [enquiries@premiercoatings.com](mailto:enquiries@premiercoatings.com)

## **4 Information security**

- 4.1 The Company will use appropriate technical and organisational measures In accordance with the Company's policies to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:
- 4.1.1 making sure that, where possible, personal information is pseudonymised or encrypted;
  - 4.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - 4.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
  - 4.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- 4.2 Where the Company uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:
- 4.2.1 the organisation may act only on the written instructions of the Company; unless otherwise instructed or engaged by you individually under a separate agreement.
  - 4.2.2 those processing the data are subject to a duty of confidence;
  - 4.2.3 appropriate measures are taken to ensure the security of processing;
  - 4.2.4 sub-contractors are only engaged with the prior consent of the Company and under a written contract;

- 4.2.5 the organisation will assist the Company in providing subject access and allowing individuals to exercise their rights under the GDPR;

the organisation will assist the Company in meeting its GDPR obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments.

## **5 Storage and retention of personal information**

- 5.1 Personal information (and sensitive personal information) will be kept securely in accordance with the Company's [*information security guide*].
- 5.2 Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow the Company's [*records retention guide*] which set out the relevant retention period, or the criteria that should be used to determine the retention period. Where there is any uncertainty, staff should consult our external advisors.
- 5.3 Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

## **6 Data breaches**

- 6.1 A data breach may take many different forms, for example:
  - 6.1.1 loss or theft of data or equipment on which personal information is stored;
  - 6.1.2 unauthorised access to or use of personal information either by a member of staff or third party;
  - 6.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;
  - 6.1.4 human error, such as accidental deletion or alteration of data;
  - 6.1.5 unforeseen circumstances, such as a fire or flood;
  - 6.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
  - 6.1.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.
- 6.2 The Company will:
  - make the required report of a data breach to the Information Commissioner's Office without undue delay, if it is likely to result in a risk to the rights and freedoms of individuals; and
  - notify the affected individuals, if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law