Policy date: 17 May 2018

Profixed Interiors Ltd Data Handling Policy

1 Policy statement

1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our business activities we will collect, store and process personal data about our employees, potential employees, former employees and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

1.3 Section 3 of this policy sets out the meanings of some of the phrases we use throughout it. These are the basic concepts and definitions set out in data protection legislation which you will need to be aware of.

2 About this policy

2.1 The types of personal data that Profixed Interiors Ltd (referred to as "**we**", "**our**" or "**us**" in this policy) may be required to handle include information about employees, potential employees, former employees and other third parties that we communicate with or receive information about. The personal data, which may be held on paper or on a computer or other media, is currently subject to certain legal safeguards specified in the Data Protection Act 1998 (the "**Act**") and other regulations.

2.2 On 25 May 2018, the Act will be replaced with the General Data Protection Regulations (the "**Regulations**"). The Regulations increase our obligations in respect of the personal data we hold and process. We want you to be aware of the Regulations as we are committed to complying with them and have begun preparing for their compliance in advance of the 25 May 2018.

2.3 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.4 This policy replaces any previous data handling policies in force at Profixed Interiors Ltd.

2.5 This policy does not form part of any employee's contract of employment and may be amended at any time. We will usually give you notice of amendments to this policy.

2.6 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.7 The Data Protection Compliance Manager is responsible for ensuring compliance with the Act (whilst applicable), the incoming Regulations and with this policy. That post is held by the Company Secretary, 07812 047261, claire@profixedinteriors.co.uk. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager.

3 Definition of data protection terms

3.1 **Data** is information which is stored, for example, electronically, on a computer, or in paper-based filing.

3.2 **Data subjects** for the purpose of this policy includes an identified or identifiable natural person.

3.3 **Personal data** means any information relating to a data subject or from which a data subject can be directly or indirectly identified by. Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about the data subject, their actions or behaviour. Please be aware that location data and online identifiers such as IP addresses also constitute personal data.

3.4 **Data controllers** are the people/organisations which determine the purposes for which, and the manner in which, personal data is processed. We are the data controller of all personal data used in our business for our own commercial purposes.

3.5 **Data users** are those of our employees and staff whose work involves processing personal data. Data users must protect the data they handle in accordance with this policy at all times.

3.6 **Data processors** include any person or organisation that is not a data user and which processes personal data on our behalf and on our instructions. We will in some circumstances be a data processor in relation to personal data provided to us by third parties if we are processing the data on their behalf.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Special categories of personal data** are categories of personal data which additional regulations apply to and include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4 Data protection principles

4.1 Anyone processing personal data must comply with the following principles. Personal data must be:

4.1.1 Processed lawfully, fairly and in a transparent manner.

4.1.2 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

4.1.3 Adequate, relevant and limited to what is necessary in relation to those purposes.

4.1.4 Accurate and where necessary, kept up to date.

4.1.5 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.

4.1.6 Processed in a manner that ensures appropriate security of the personal data.

4.2 As a data controller, it is our responsibility to demonstrate compliance with those principles.

4.3 **Under no circumstances should personal data be processed in breach of the above principles. Please contact the Data Protection Compliance Manager whose details are set out in clause 2.7 if you think there may have been a breach of the above principles.**

4.4 In addition to the above principles, personal data must not be transferred outside of the European Economic Area ("**EEA**") without satisfying certain criteria.

It is our policy that no-one processing personal data within our organisation should transfer data outside of the EEA without the data subjects' explicit consent. In order to be able to transfer personal data outside of the EEA, we must ensure:

4.4.1 We have explained to the data subject why we wish to transfer their data outside of the EEA;

4.4.2 We have explained to the data subject the ramifications of sending the personal data outside of the EEA, for example, that the third party country may not have as protective data protection legislation which could result in personal data being used for purposes for which it was not provided;

4.4.3 The data subject has given consent to the specific transfer and the specific purposes for which the data will be used;

4.4.4 The data subject has given a clear and unambiguous indication of their consent.

4.5 We must be able to demonstrate that the data subject provided their compliant explicit consent to transfer their personal data outside of the EEA and so telephone notes or emails demonstrating the data subject's explicit consent must be made or retained.

4.6 **Under no circumstances is personal data to be transferred outside of the EEA without compliant consent of the data subject or authority of the Data Protection Compliance Manager whose details are set out in clause 2.7.**

5 Processed lawfully, fairly and in a transparent manner

5.1 This principle is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, the personal data must be processed on the basis of one of the legal grounds set out:

5.2.1 For processing carried out before 25 May 2018, in the Act; and

5.2.2 For processing carried out on or after 25 May 2018, in the Regulations.

Where processing personal data in the course of our business, we will ensure that one of those grounds is met or we will not process the personal data. The grounds include, among others:

5.2.2.1 the data subject has given their consent to the processing for one or more specific purposes;

5.2.2.2 the processing is *necessary* for the performance of a contract to which the data subject is a party to or for pre-contractual steps taken at the individual's request;

5.2.2.3 the processing is *necessary* for compliance with a legal obligation to which the data controller is subject;

5.2.2.4 the processing is *necessary* in order to protect the vital interests of the data subject or of another natural person.

5.2.2.5 the processing is *necessary* for the legitimate interest of the data controller or a third party except where those interests are overridden by the interests and rights of the data subject.

5.2.3 As set out in section 4 above, where the ground for processing depends on whether the processing is "*necessary*" or not, this

imposes a strict requirement on us, the ground will not be met if we can achieve the purpose of the processing by some other reasonable means or the processing is only "*necessary*" because of a way in which we have decided to operate our business. **You must consult the Data Protection Compliance Manager whose details are set out in clause 2.7 if you are unsure whether or not a lawful ground for processing has been met.**

5.3 Where we want to process any special categories of personal data, one of the following must be satisfied otherwise we must not process that special category of personal data:

5.3.1 the data subject has given explicit consent to the processing of those personal data for one or more specific purposes;

5.3.2 the processing is *necessary* for the purposes of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment and social security and social protection law;

5.3.3 the processing is *necessary* to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

5.3.4 the processing relates to personal data which are manifestly made public by the data subject;

5.3.5 the processing is *necessary* for the establishment, exercise or defence of legal claims;

5.3.6 the processing is *necessary* for the purposes of assessment of the working capacity of the employee.

Again, where the term "*necessary*" is used, section 5.2.3 above applies.

6 Collected for specified, explicit and legitimate purposes

6.1 In the course of our business, we may collect and process a variety of personal data including, for example, employees' and potential employees' CVs, passport details, addresses and bank account details, emergency contact details, statement of health, GP medical notes, vehicle and driving licence details.

6.2 We may receive personal data directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise]) and data we receive from other sources (including, for example, contractors, sub-contractors, limited sole traders, recruitment agencies and others.

6.3 We will only process personal data for the specific purposes for which it was collected or for any other purposes specifically permitted by the Act or the

Regulations (as applicable)]. For example, if we collect a customer's email address to assist the customer with a product issue only, we must not then add that email address to our marketing database.

6.4 We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7 Adequate, relevant and limited to what is necessary

7.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject and will not collect more personal data than we need in relation to that specific purpose.

8 Accurate and up to date data

8.1 We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

9 Timely processing

9.1 We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

10 Data security

10.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

10.2 We have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

10.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

10.3.1 **Confidentiality** means that only people who are authorised to use the data can access it.

10.3.2 **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

10.3.3 **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal

data must therefore be stored on Profixed Interiors Ltd central computer system instead of individual PCs.

10.4 Security procedures include:

10.4.1 **Entry controls.** Our offices are entry controlled. Any stranger seen in our offices or the entry-controlled areas should be reported.

10.4.2 **Secure lockable desks, cupboards and filing cabinets.** Desks, cupboards and filing cabinets should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

10.4.3 **Methods of disposal.** Paper documents containing personal data should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

10.4.4 **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

10.4.5 **Digital devices:**

10.4.5.1 Your personal digital devices:

(a) Profixed Interiors Ltd's computer system must only be accessed using your secure login details;

(b) you may access the secure login portal from your own personal devices, but you are not permitted to download anything from the portal to your desktop (or equivalent) or send work emails from your personal accounts.

10.4.5.2 Digital devices:

(a) all of our mobiles and laptops must be encrypted and password protected and the passwords must be changed every 6 months you must ensure that your work issued mobile devices have the "Find My iPhone" app or equivalent installed to assist in locating lost devices or to allow the content to be erased if the device cannot be found.

11 Notifying data subjects

11.1 If we collect personal data directly from data subjects, we will inform them about:

11.1.1 The purpose or purposes for which we intend to process that personal data.

11.1.2 The types of third parties (e.g. suppliers or professional advisers), if any, with which we will share or to which we will disclose that personal data.

11.1.3 The means by which, if any, data subjects can limit our use and disclosure of their personal data (e.g. by unsubscribing from our emails or changing their account settings).

11.2 If we receive personal data about a data subject from other sources and we haven't previously provided the data subject with a privacy notice which notifies the data subject about those types of other sources, we will provide the data subject with the information in 11.1 as soon as possible thereafter.

11.3 Where relevant, we will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

12 Data subject's rights

12.1 We will process all personal data in line with data subjects' rights, in particular their right to:

12.1.1 Request information on what personal data we hold about them and provide access to it.

12.1.2 Prevent the processing of their data for direct-marketing purposes.

12.1.3 Ask to have inaccurate data amended, erase data we hold about them or restrict the types of process we carry out in respect of that data.

12.1.4 Request we provide the personal data we hold about them in order they can use it for their own purposes across other services.

If the data subjects exercise any of their above rights, before doing anything, please contact the Data Protection Compliance Manager whose details are set out in clause 2.7 immediately in order they can assist you with how to proceed.

When receiving enquiries, we must not disclose personal data we hold on our systems unless we have check the enquirer's identity to make sure that information is only given to a person who is entitled to it.

Employees should not be coerced into taking action in relation to a data subjects' personal information under any circumstances without being sure it is appropriate to do so as this in itself could result in a breach of the applicable legislation.

13 Changes to this policy

13.1 We reserve the right to change this policy at any time.