Introduction

The General Data Protection Regulation (GDPR) is a pan-European regulation, which is effective as of 25 May 2018. On the same day, the UK's Data Protection Bill will be passed into law, as the Data Protection Act 2018, effectively implementing the GDPR into UK law.

Oracle Environmental Experts Ltd (OEE) receives, uses and stores personal information about our clients, customers, sub-contractors and employees. It is important that this information is handled lawfully and appropriately in line with the requirements of the Data Protection Act and the General Data Protection Regulation (collectively referred to as the 'Data Protection Requirements').

We take our data protection duties seriously, because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

About This Policy

This policy, and any other documents referred to in it, sets out the basis on which we will process any personal data we collect as part of our business operations.

This policy does not form part of any employee's contract of employment and may be amended at any time.

Dr Diane Green is the Data Protection Compliance Manager within the organisation and is responsible for ensuring compliance with the Data Protection Requirements and with this policy.

What is Personal Data?

- *Personal data* means data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession).

- *Processing* is any activity that involves use of personal data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

- *Sensitive personal data* includes personal data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offences or convictions. Sensitive personal data can only be processed under strict conditions, including with the consent of the individual.

Data Protection Principles

Anyone processing personal data, must ensure that data is:

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

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

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

d) 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;

e) Kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed;

f) 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.

g) Not transferred to people or organisations situated in countries without adequate protection and without firstly having advised the individual.

Fair and Lawful Processing

The Data Protection Requirements are 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 individual.

In accordance with the Data Protection Requirements, we will only process personal data where it is required for a lawful purpose. The lawful purposes include (amongst others): whether the individual has given their consent, the processing is necessary for performing a contract with the individual, for compliance with a legal obligation, or for the legitimate interest of the business. When sensitive personal data is being processed, additional conditions must be met.

Processing for Limited Purposes

In the course of our business, we may collect and process the personal data that we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, e-mail or otherwise) and data we receive from other sources (including, for example, site location data, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

We will only process personal data for the purposes specifically permitted by the Data Protection Requirements. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

Notifying Individuals

If we collect personal data directly from an individual, we will inform them about:

a) The purpose for which we intend to process that personal data, as well as the legal basis for the processing.

b) Where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued.

c) The types of third parties, if any, with which we will share or disclose that personal data.

d) The fact that the business intends to transfer personal data to a non-EEA country or international organisation and the appropriate and suitable safeguards in place.

e) How individuals can limit our use and disclosure of their personal data.

f) Information about the period that their information will be stored or the criteria used to determine that period.

g) Their right to request from us as the controller access to and rectification or erasure of personal data or restriction of processing.

h) Their right to object to processing and their right to data portability.

i) Their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn.

j) The right to lodge a complaint with the Information Commissioners Office (ICO).

k) Other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources.

l) Whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data.

m) If we receive personal data about an individual from other sources, we will provide them with this information as soon as possible (in addition to telling them about the categories of personal data concerned) but at the latest within 1 month.

We will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

Adequate, Relevant and Non-Excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

Accurate Data

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.

Timely Processing

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

Processing in line with Data Subject's Rights

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

a) Confirmation as to whether or not personal data concerning the individual is being processed.

b) Request access to any data held about them by a data controller.

c) Request rectification, erasure or restriction on processing of their personal data.

d) Lodge a complaint with a supervisory authority.

e) Data portability.

f) Object to processing including for direct marketing.

g) Not be subject to automated decision making including profiling.

Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

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

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

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

c. **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on OEE's 'G Drive' central computer system instead of individual PCs. All computers must be password protected and the use of portable external drives will not be permitted.

Changes to this Policy

We reserve the right to change this policy at any time. Where appropriate, we will notify changes by mail or email.

This policy has immediate effect and replaces previous versions. This policy will be reviewed and amended, as necessary.

Signed DGreen Diane Green, Director

Version 5 Issued May 2022