Personal Data Protection Policy

As a responsible company, Environmental Solutions through Partnership Ltd (ESP) takes the protection of personal data extremely seriously. The following policy details how ESP adheres to the General Data Protection Regulation (GDPR).

It should be noted that we have not appointing a Data Protection Officer (DPO) as we are neither a public authority nor have core activities that require large scale, regular and systematic monitoring of individuals. However, ESP does have sufficient staff and resources to discharge our data protection obligations under GDPR.

1.0 Principles

ESP adheres to the following principles as set out by GDPR.

Data will be:

a. Processed lawfully, fairly and in a transparent manner.
b. Collected for specified, explicit and legitimate purposes – i.e. it is necessary.
c. Adequate, relevant and limited to what is necessary.
d. Accurate and, where necessary, kept up to date.
e. Kept in a form which permits identification of subjects for no longer than is necessary.
f. Processed in a manner that ensures appropriate security of the personal data.

2.0 Lawful basis

ESP will only process personal data if it has one of the following lawful bases to do so:

a. Consent.
b. Contract.
c. Legal obligation.
d. Vital interest.
e. Public task.
f. Legitimate interest

ESP will determine and document our lawful basis before we begin processing personal data.

3.0 Rights of the Individual

ESP will uphold the rights (as appropriate) of the individual as follows:

a. The right to be informed.
b. The right of access.
c. The right to rectification.
d. The right to erasure.
e. The right to restrict processing.
f. The right to data portability.
g. The right to object.

Privacy Information & Notices

ESP will notify individuals for whom we hold personal data of the following:

- Our purposes for processing their personal data.
- Our lawful basis for processing their personal data.
- Our personal data retention periods.
- Who their personal data will be shared with, if at all.

Access

ESP will allow access to a subject's personal data upon request by the individual.

Rectification

ESP will consider any request to rectify personal data if a request is made either verbally or in writing. ESP will respond to any request within one calendar month.

Erasure

ESP will consider any request to erase personal data if a request is made either verbally or in writing. This is 'the right to be forgotten'. ESP will respond to any request within one calendar month.

Processing Restriction

ESP will consider any request to restrict the processing of personal data if a request is made either verbally or in writing. ESP will respond to any request within one calendar month.

Data Portability

ESP will consider any request to port personal data if a request is made either verbally or in writing. ESP will respond to any request within one calendar month.

Objection

If ESP holds personal data on the basis of Legitimate Interest, ESP will consider not processing that personal data if an objection is made either verbally or in writing. ESP will respond to any request within one calendar month.

4.0 Accountability & Governance

As a data controller, ESP will only appoint data processors who can provide sufficient guarantees that the requirements of the GDPR will be met. Processors must only act on the documented instructions of ESP and there will be contractual agreements in place to ensure that both parties understand their respective responsibilities and liabilities.

ESP will maintain documentation of our processing activities, to include:

- The purposes of our data processing.
- Descriptions of the categories of personal data held.

- The categories of recipients of personal data.
- Transfers to other countries including the transfer mechanism safeguards in place.
- Retention schedules.
- Information required for privacy notices.
- Records of consent.
- Location of personal data.

ESP will also:

- Implement appropriate security measures to ensure confidentiality, integrity and availability of personal data.
- Record and, where necessary, report personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible.
- Conduct data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests.

5.0 Payments on website

For customers who choose to make payment by credit or debit card, ESP utilise Worldpay to process this data. Details of a card are held securely within the Worldpay interface. In order to facilitate this payment method, ESP has applied for and has been granted the status of being PCI DSS compliant until 11th January 2019.

Andrew C Fletcher
Director