ESP UTILITIES GROUP LTD

Data Protection Policy

Document Details Data Protection Policy			
Version	V1.51	**Classification**	INTERNAL
Author	Legal & Contracts Manager		
Reviewed by	Business Operations Director (VS)	**Last Reviewed**	December 2023
Approved by	Senior Management Team	**Approval date**	March 2024
Review Frequency	Yearly	**Next Review Date**	December 2024

Version history				
Version	**Date**	**Author**	**Reason for new version**	**Sections affected**
0.01	05/11/14	ISM (JB)	-	-
0.02	24/11/14	Business Operations Director (VS)	Addition of Appendix 1 referencing Data Access Requests	Appendix 1
1.0	25/11/14	Business Operations Director (VS)	Senior Management Review	None
1.1	30/04/18	Legal & Contracts Manager (JR)	Implementation of Regulation EU 2016 / 679 (the General Data Protection Regulation),	All
1.2	October 2020	Legal and Contracts Manager (EW)	Annual review and update	all
1.3	December 2021	Legal and Contracts Manager (EW)	Annual review and update	All
1.31	December 2022	Junior Legal Counsel (OK)	Annual review and update	All
1.4	October 2023	Junior Legal Counsel (OK)	Update to version number only.	Version History

1.41	December 2023	Junior Legal Counsel (OK)	Annual Review Addition of all the lawful bases of processing.	All
1.5	December 2023	Junior Legal Counsel (OK)	Publication following annual review & updates. Addition of all the lawful bases of processing.	All
1.51	March 2024	Junior Legal Counsel (OK)	Incorporating the “Appropriate Policy” document provisions.	All

1. Objective

ESP collects and uses information about customers, consumers, potential customers, householders, employees, and other individuals to carry out its day-to-day business. ESP is registered with the Information Commissioner's Office as a Data Controller and a Data Processor. This policy applies to all personal data; however it is collected, recorded, and used – whether on paper, in a computer storage system or recorded on other material.

Additionally, we process Special Category data in accordance with Article 9 of the UK General Data Protection Regulation (UK GDPR) and Schedule 1 of the Data Protection Act (2018).

The objective of this policy is to ensure ESP Utilities Group Ltd and its group companies ("ESP") comply with the Data Protection Act 2018 (as amended) ("DPA") which sets out the data protection framework in the UK and define what Special Category data we process, our lawful basis for processing that data, the purposes for which we process it, and how we ensure compliance with the principles of data protection law provided in Article 5 of the UK GDPR.
The DPA enacts the GDPR into UK law and tailors how the GDPR applies in the UK; it is commonly referred to as the UK GDPR.

2. UK GDPR

2.1 What does it do

The Data Protection Act 2018 controls how personal data information is used by organisations, businesses or the government. Everyone responsible for using personal data is required to follow strict rules called 'data protection principles' ensuring the information is:

- used fairly, lawfully and transparently;
- used for specified, explicit purposes;
- used in a way that is adequate, relevant and limited to only what is necessary;
- accurate and, where necessary, kept up to date;
- kept for no longer than is necessary;
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

There is stronger legal protection for more sensitive information ('special category data');. sensitive information includes:
race;

- ethnic background;
- political opinions;
- religious beliefs;
- trade union membership;
- genetics;
- biometrics (where used for identification);
- health;
- sex life or orientation.

2.2 Why does the UK GDPR matter?

Penalties for non-compliance with the UK GDPR regarding the collection and use of personal data are potentially devasting.

Failure to comply may attract a fine of €20 million or 4% of the total company annual turnover, whichever is greater; this remains in line with EU GDPR provisions. The most likely source of risk is by either a data incident, a whistle-blower or a competitor.

2.3 What is personal data and the legal bases for processing it?

Personal data is defined as any information related to a natural person that can be used to identify that person directly or indirectly; with that person being called a 'data subject'.

There are eight (8) legal bases for processing personal data and these are:

- **Consent** – if consent is relied upon, companies must seek consent from Data Subjects to handle their personal data in a clear fashion, giving the data subject a real choice. Consent requires a positive opt-in; pre-ticked boxes and other default methods of consent cannot be relied upon.
- **Contract** – can be relied upon to process an individual's personal data to deliver a contractual service or because an individual has asked for something to be done before entering into a contract.
- **Legal obligation** – this can be relied upon if there is a need to process personal data to comply with common law or statutory obligation. This does not apply to contractual obligations.
- **Vital Interests** – this is likely to be relied upon if there is a need to process an individual's personal data to protect an individual's life.
- **Public Task** – this can be relied upon to process personal data 'in the exercise of official authority', this covers public functions and powers that are set out in law or to perform a specific task in the public interest that is set out in law. This is most relevant to public authorities but can also apply to any organisation that exercises official authority or carries out tasks in the public interest.
- **Legitimate Interest** – this is likely to be most appropriate where and individuals' personal data is used in ways that the individual would reasonably expect, which have a minimal privacy impact or where there is a compelling justification for the processing. Relying on this basis brings an extra responsibility to consider and protect an individual's rights and interests. There are three elements to this basis which must be reviewed before it is relied upon and these are:
  The Purpose Test: are you pursuing a legitimate interest?
  The Necessity Test: is the process necessary for that purpose?
  The Balancing Test: do the individual's interests override the legitimate interest?
- The last two bases are in relation **Special Category Data** and **Criminal Offence Data** which require one of the legal bases set out above along with a legal basis listed in Article 9 of the UK GDPR and/or additional conditions and safeguards set out in Schedule 1 of the DPA 2018.

Whichever legal basis is relied upon, processing must be necessary and if the end goal can be achieved without processing personal data, the legal basis for processing will not apply.
The decision to rely on a specific lawful basis must be documented and the reasoning must be justifiable.

Additionally, for the processing of children's data, UK GDPR requires explicit consent from the parents or guardians if the child is under the age of 13.

2.4 Summary of the 7 Data Protection Principles

(a) Lawful, fair and transparent processing – this means that in processing personal data, ESP must do so:
   (i) *Lawfully - means all processing should be based on a legitimate purpose;*
   (ii) *Fairly* – means companies take responsibility and do not process data for any purpose other than the legitimate purposes; and
   (iii) *Transparently* – means that companies must inform data subjects about the processing activities on their personal data.

(b) **Limitation of purpose, storage and data minimisation** – ESP is expected to limit processing, collect only the data which is necessary, and not keep personal data once the processing purpose is completed. This would effectively bring the following requirements:
   (i) Forbid processing of personal data outside the legitimate purpose for which the personal data was collected;
   (ii) Mandate that no personal data, other than what is necessary, be requested;
   (iii) Ensure that the personal data is deleted once the legitimate purpose for which it was collected is fulfilled.

(c) **Accuracy** – information must be kept 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.

(d) **Integrity and Confidentiality (Security)** – data must be 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.

(e) **Accountability** – ESP is responsible for and must be able to demonstrate compliance with the above provisions.

2.5 Individual Rights

Data Subject Rights

the Data Subjects have been assigned the right to ask the company what information it has about them, and what the company does with this information. In addition, a data subject has the right to ask for correction, object to processing, lodge a complaint, or even ask for the deletion or transfer of his or her personal data.

2.6 ESP's Lawful basis for processing

As and when the company has the intent to process personal data beyond the **legitimate** process for which the data was collected, a clear and explicit **consent** must be asked from the data subject. Once collected, this consent must be documented. The data subject is allowed to withdraw consent at any point.

Consent requires a positive opt-in and must be a very clear and specific statement of consent requested separately from any other terms and conditions that may apply.

2.7 Special Category data – To be read with Appendix 2

We process the following types of Special Category data:

- Data concerning health.

2.7.1 Schedule 1 DPA 2018 conditions for processing

Below we have listed the Schedule 1 conditions upon which we are relying,

- Schedule 1, Part 2, para 8 (equality of opportunity or treatment), where ESP needs to process Special Category data for the purposes of performing its obligations in managing the Priority Service Register and any obligations stemming from it.

Further details on ESP's obligations in processing special category data are contained in Appendix 2.

2.8 **Personal Data Breaches** – organisations must maintain a Personal Data Breach Register and based on the severity, the regulator and data subjects should be informed within 72 hours of identifying the breach.

2.9 **Privacy by Design** – companies should incorporate organisational and technical mechanisms to protect personal data in the design of new systems and processes; that is, privacy and protection aspects be included by default.

2.10 **Data Protection Impact Assessment** – this needs to be conducted when a significant change is introduced in the processing of personal data.

2.11 **Data Transfers** – the controller of personal data has the accountability to ensure that personal data is protected and UK GDPR requirements respected. This means controllers have the obligation to ensure the protection and privacy of personal data

2.12 **Data Protection Officers** – when there is significant processing of personal data an organisation should assign a Data Protection Officer. When assigned, that DPO would have the responsibility of advising the company about compliance with UK GDPR requirements.

2.13 **Awareness and training** – organisations must create awareness among employees about the key UK GDPR requirements and conduct regular training.

3. Responsibilities

ESP's Business Operations Director is nominated as ESP's data protection officer, responsible for monitoring and managing the systems and processes used to share information with suppliers and industry partners and for advising ESP management and employees on the implementation of this policy.

Line Managers are responsible for ensuring that staff comply with this and related policies.

All staff and other authorised users are responsible for ensuring that the principles of this policy are followed in the course of day-to-day activities.

4. Compliance

4.1 Key Principles

(a) The Company will apply, through appropriate management, strict application of these criteria and controls: Observe fully, conditions regarding the fair collection and use of information.
(b) Meet its legal obligations to specify the purposes for which information is used.
(c) Collect and process appropriate information, only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
(d) Ensure the quality of information collected and processed.
(e) Apply checks to determine the length of time information is held.

(f) Ensure that the rights of people about whom information is held, can be fully exercised in accordance with the Data Protection Legislation.
(g) Take and maintain appropriate technical and organisational security measures to safeguard personal information.
(h) Ensure that personal information is not transferred abroad without suitable safeguards and appropriate consents and permissions.
(i) Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
(j) Set out clear procedures for responding to requests for information.
(k) Ensure that personal information is only processed in a manner which is lawful.

4.2 Additional applications

(a) There is someone with specific responsibility for Data Protection.
(b) Everyone managing and handling personal information understands that they are legally and contractually responsible for following good data protection practice.
(c) Everyone managing and handling personal information is appropriately trained to do so.
(d) Everyone managing and handling personal information is appropriately supervised.
(e) Anybody wanting to make enquiries about handling personal information knows what to do.
(f) Queries about handling personal information are promptly and courteously dealt with.
(g) Methods of handling personal information are clearly described.
(h) A regular review and audit is made of the way personal information tis held, managed and used.
(i) Methods of handling personal information are regularly assessed and evaluated.
(j) Performance of those handling personal information is regularly assessed and evaluated.

4.3 Collection and Use of Data

ESP will only collect data which is required to allow it to carry out its business. All data subjects will, at the time of collection, be notified of each purpose to which the data is put, the duration it will be held for, and the lawfulness of processing, and no additional data will be collected or stored by ESP.

4.4 Maintaining and Destroying Data

ESP will ensure that all personal data will be stored correctly and securely within its Information Security Management System (ISMS) during the time the data is required by the company. Once the data is no longer required the data will be returned, deleted or destroyed, in accordance with the ESP **Information Asset Management Policy (ID-POL)** and **Data Retention Policy**.

4.5 Access Requests

Any individual has the right to access, correct, restrict, and transfer their personal information. An individual can send ESP, in its capacity as data controller a subject access request requiring ESP to advise the individual about the personal information ESP holds about them, where the information was obtained from, and who it is shared with, and to provide them with a copy of that information. ESP will ensure it responds to all requests in accordance with the UK GDPR. More details regarding ESP's obligation to respond to data access requests are contained in Appendix 1 which is to be read in conjunction with the **Data Subject Request Handling Policy** and the **Data Subject Request Handling Procedure**.

4.6 Reporting

All staff should report immediately to their line manager in the first instance any observed or suspected incidents where this policy has been breached, so that an investigation into the potential loss can be carried out and procedures can be improved.

In the event that a breach is detected, the Data Protection Officer shall, within the time-frames set out in the Data Protection Legislation, assess the seriousness of the breach and determine whether it is necessary to notify the Information Commissioner's Office or the Information Commissioner's Office and the impacted data subject(s).

5. Record of Processing Activities (ROPA)

ESP's ROPA is managed and maintained by the Legal Counsel with the support of relevant departmental representatives. Collectively, there is a responsibility to ensure personal data processing activities are recorded and regularly reviewed.

6. Advice and Assistance

Advice on the implementation of this policy can be obtained from the ESP Information Security Manager (Andrew Martin) Andrew Martin, Data Protection Officer (Vicki Spiers) or the Legal team.

Appendix 1

Requests for Information

Data Subjects (individuals about whom data is held on record) can request access to, rectification, deletion, transfer, and confirmation of the personal information processed by ESP, outside of normal business processes.

Upon receipt of such request, ESP will take reasonable steps to confirm that identity of the Data Subject, and ESP shall, without undue delay, and in any case within 30 days, respond to the request. Such information will be provided free of charge, unless the requests are manifestly unfounded, excessive or repetitive, in which case ESP shall be entitled to;

a. Charge a reasonable fee, considering the administrative costs providing the information or communication or taking the action requested; or
b. Refuse to act on the request.

Data access request should be passed for handling to the Business Operations Director who will ensure that it is processed fairly in accordance with the Data Protection Legislation.

Responses to data access requests shall be concise, transparent, intelligible and in an easily accessible form, using clear and plain language, considering the specific characteristics of the data subject (e.g., a vulnerable customer, consumer, householder or minor). The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Appendix 2

Special Category Data Provisions

1. **How we comply with the data protection principles in Article 5 of the UK GDPR**
   Article 5(2) of the UK GDPR requires Data Controllers to demonstrate how they comply with the data protection principles provided in Article 5(1). This section illustrates the measures we have taken to demonstrate accountability for the personal data we process and contains details about how we ensure compliance with the principles of the UK GDPR.

2. **Accountability**
   To comply with the data protection principles provided in Article 5 of the UK GDPR we have developed the following measures and documents:
   - We have appointed a Data Protection Officer whose role and responsibilities align with the provisions of Articles 37-39 of the UK GDPR.
   - Our Record of Processing Activities sets out the personal data categories we process, the purposes, the lawful bases under Article 6 and Article 9 UK GDPR, our retention periods for the data, recipients of personal data, any international transfers of data and our means of keeping data secure.
   - Our Privacy Notices explain to individuals how and why their data is processed by ESP, what their rights are, and how they can get in touch with our DPO and the ICO.
   - When we routinely and/or regularly share data with third parties, we enter into written agreements with Data Controllers and Data Processors which meet the provisions of Articles 26 and 28 of the UK GDPR respectively.
   - We carry out Data Protection Impact Assessments (DPIAs) for uses of personal data that are likely to result in a risk to individuals' data protection rights and freedoms.
   - We implement appropriate security measures which are proportionate to the risks associated with the processing.

3. **Lawful, fair and transparent processing**
   - We provide clear and transparent information to individuals about why we process their personal data, including our lawful basis, in our Privacy Notices. This includes information about why we process Special Category data.
   - We need to process Special Category Data for the substantial public interest conditions outlined in section 3 of this policy to meet the requirements of legislation such as the Electricity (Standards of Performance) Regulations 2015.
   - We process employment data to meet our legal obligations as an employer.

3.1 Purpose limitation

We process Special Category data only where it is necessary to do so for specified purposes. We only process Special Category data where we have a lawful basis to do so under Articles 6, 9 and 10 UK GDPR and, where required, when we have identified a condition under Schedule 1 DPA 2018.

We will not process any Special Category data for purposes which would be incompatible with the purpose for which the data was originally collected.

3.2 Data minimisation

We design our data collection forms and other data collection tools to ensure that we only collect the Special Category data necessary to achieve the relevant purpose. Our purposes are set out in our Privacy Notices.

We collect and retain Special Category data only for long enough to fulfil our purposes. We collect enough but no more than we need in accordance with the data minimisation principle, and we only hold Special Category data for the period set out in our retention policies.

Our retention schedule sets out the correct disposal action once records containing special category data are no longer required.

3.3 Accuracy

When we identify data which is inaccurate or out of date, having due regard for the purpose for which the data was processed, we will take necessary steps to rectify or erase it without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

3.4 Storage limitation

Special Category data processed by us for the purpose of employment or substantial public interest will be retained for the periods set out in our retention schedule. The retention policy for record categories is determined by our legal and regulatory obligations, and our business requirements.

3.5 Security

Electronic data is hosted on a secure network, and on the secure servers of third-party cloud storage providers with whom we have contractual agreements. Electronic and hard copy data is managed according to our internal records management policies and procedures.