# DATA PROTECTION POLICY

## DOCUMENT INFORMATION

| | | | | | |
|---|---|---|---|---|---|
| Classification | External | Version Number | 0.1 | Status | FINAL |
| Valid From | 30/9/23 | Approved By | Adindu Nwichi | Prepared By | Bulletproof |
| DATE NEXT REVIEW DUE | 30-9-2024 | | | | |

## VERSION HISTORY

| Date | Version Number | Name | Change Description |
|---|---|---|---|
| 15/09/2023 | 0.1 | Adindu Nwichi | Initial Document Creation |
| 17/10/23 | 0.2 | Tina Morley | Formatting |

## CONTENTS

## 1. PURPOSE

The purpose of this policy is to set out East Suffolk Services Limited (ESSL)'s approach to data protection and data privacy.

## 2. INTRODUCTION

ESSL delivers a range of crucial services, on behalf of East Suffolk Council. These include Waste and Recycling Collections, Grounds Maintenance, Street Cleansing, Facilities Management, CCTV, Home Alarms and Parking Enforcement.

The personal data that ESSL processes to provide these services relates to its client's and other individuals as necessary, including staff.

ESSL processes the personal data of staff and customers and is committed to ensuring that all the personal data that it processes is carried out in accordance with all data protection law.

ESSL ensures that good data protection practice is embedded in the culture of our staff and our organisation.

ESSL's other data protection policies and procedures are:

- record of processing activities
- privacy notices (website, employees)
- personal data breach reporting process and a breach register
- data retention policy
- data subject rights procedure
- data protection impact assessment process

'Data Protection Law' includes the General Data Protection Regulation 2016/679; the UK Data Protection Act 2018 and all relevant UK data protection legislation.

## 3. SCOPE

This policy applies to all personal data processed by and is part of ESSL's approach to compliance with data protection law. All ESSL staff, partners or third parties who have, or may have access to personal data are expected to have read, understood and comply with this policy and failure to comply may lead to disciplinary action for misconduct, including dismissal or contract termination.

## 4. RESPONSIBILITIES

ESSL is a data controller and data processor under the GDPR/DPA 2018.

All managers are responsible for ensuring personal data is handled in accordance with ESSL's policies and procedures and for encouraging best practice in the handling of personal data.

- The DPO is accountable to the Board of Directors and for ensuring compliance with data protection law can be demonstrated.
- Compliance with data protection law is the responsibility of all employees, partners and third parties working on behalf of ESSL.
- The Director (Performance & Improvement) is ultimately accountable for ensuring ESSL is compliant with data protection law.

ESSL will ensure that all staff, partners or third parties who handle personal data on its behalf are aware of their responsibilities under this policy and other relevant data protection and information security policies, and that they are adequately trained and supervised. Breaching this policy may result in disciplinary action for misconduct, including dismissal or contract termination. Obtaining (including accessing) or disclosing personal data in breach of ESSL's data protection policies may also be a criminal offence.

## 5. DATA PROTECTION PRINCIPLES

ESSL complies with the data protection principles set out below. When processing personal data, it ensures that:

- it is processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

- it is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')

- it is all adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

- it is all accurate and, where necessary, kept up to date and that reasonable steps will 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 ('accuracy')

- it is 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 ('storage limitation')

- it is 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 ('integrity and confidentiality')

- It is responsible for complying with the data protection principles and will demonstrate this in accordance with Article 5(2) "Accountability" by implementing policies and procedures, technical and organisational measures and keeping documentation such as breach records and DSAR records.

## 6. DATA SUBJECT RIGHTS

ESSL has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under data protection law. All staff have received training and are aware of the rights of data subjects. Staff can identify such a request and know who to send it to. Refer here to find the Data Subject Rights Request Procedure.

All requests will be considered without undue delay and satisfied within one calendar month of receipt as far as possible.

ESSL will ensure the rights as detailed below can be exercised by data subjects

**Informed:** The right to be informed about the collection and use of personal data is addressed via company privacy notices.

**Subject access:** the right to request information about how personal data is being processed, including whether personal data is being processed and the right to be allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:

- the purpose of the processing
- the categories of personal data
- the recipients to whom data have been disclosed or which will be disclosed
- the retention period
- the right to lodge a complaint with the Information Commissioner's Office
- the source of the information if not collected direct from the subject, and
- the existence of any automated decision-making.

**Rectification:** the right to allow a data subject to rectify inaccurate personal data concerning them.

**Erasure:** the right to have data erased and to have confirmation of erasure, but only where:

- the data is no longer necessary in relation to the purpose for which it was collected, or
- where consent is withdrawn, or
- where there is no legal basis for the processing, or
- there is a legal obligation to delete data.

**Restriction of processing:** the right to ask for certain processing to be restricted in the following circumstances:

- if the accuracy of the personal data is being contested, or
- if our processing is unlawful but the data subject does not want it erased, or
- if the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims, or
- if the data subject has objected to the processing, pending verification of that objection.

**Data portability:** the right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if [company name] was processing the data using consent or based on a contract.

**Object to processing:** the right to object to the processing of personal data relying on the legitimate interests processing condition unless [company name] can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject or for the establishment, exercise or defence of legal claims.

**Object to automated profiling:** the right to object where solely automated decision-making is being carried out that has legal or similarly significant effects on the data subject.

## 7. SPECIAL CATEGORY DATA

This includes the following personal data revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
- an individual's health
- a natural person's sex life or sexual orientation
- criminal convictions or offences.

ESSL will apply additional organisational and technical measures to protect special category data where processed based on risk to the data subject.

ESSL will only process special category data where it has an Article 6 lawful basis and an Article 9 exception to do so.

## 8. CONSENT

ESSL understands the conditions of consent as defined in Article 7 of the GDPR and will ensure that:

- Consent is a specific, informed and unambiguous indication of the data subjects wishes
- The data subject can withdraw consent at any time
- Withdrawal of consent is as easy as it was to give
- Where information society services are provided to children, consent of the parent/guardian will be obtained based on the age limits defined in the country concerned
- Records of consent are kept as evidence
- The data subject is competent to give consent and is doing so freely without duress

## 9. SECURITY

ESSL will always assess the risk of processing personal data to the data subject and

- Ensure that personal data is stored securely using software that is kept-up-to-date and supported.
- Access to personal data shall be role based, limited to personnel who need access and appropriate security shall be in place to avoid unauthorised sharing of information.
- When personal data is deleted this shall be done safely such that the data is irrecoverable.
- Appropriate back-up and disaster recovery solutions shall be in place.
- Staff are given information security training and information security policies and procedures are adhered to
- Personal data is encrypted where possible at rest and in transit
- Where possible personal data is anonymised or pseudonymised
- All passwords used meet password policy requirements
- Anti-malware software is deployed on all devices handling personal data
- Paper documents containing personal data shall be stored in lockable cabinets

## 10. DATA BREACHES

ESSL is dedicated to complying with the requirements for responding to and reporting a data breach. Data breaches can come in many forms, including but not limited to:

- Insider threat
- Malware attacks
- Accidental web exposure
- Data in transit

Data breaches will be identified, and, where they present a risk to the data subject, the Information Commissioner's Office will be notified without undue delay and within 72 hours of them being discovered. Breaches will be assessed, and mitigation will be applied to ensure the breach does not continue or happen again. Data Subjects impacted by this will be notified where there is a high risk to them and/or according to the ICO advice.

## 11. DATA TRANSFERS

ESSL will ensure that any personal data transferred to third countries or third parties in third countries will not be transferred without suitable safeguards which may include:

- International Data Transfer Agreement
- Binding corporate rules
- Adequacy decision
- An exception as defined in Article 49 of the GDPR

## 12. DATA PROTECTION BY DESIGN

Data Protection by Design allows for Data Protection to be built into a business's ethos but ensuring processes, services and other ideas are risk assessed from a GDPR point of view. ESSL is committed to practising this throughout the business to ensure systems are built with data protection as the first thought, rather than an afterthought. All staff must declare new processes involving data to ensure this assessment is completed where needed.

## 13. MONITORING AND REVIEW

This policy was last updated on the date shown on the front of this procedure and shall be regularly monitored and reviewed, at least annually.