DATA PROTECTION POLICY

Contents

Introduction

As a traffic engineering and transport planning provider, we collect personal data to help operate our business and deliver our services to you. It is required to do so to comply with other legislation. It is also required to keep this data for different periods depending on the nature of the data.

This policy sets out how the Company implements the Data Protection Laws. It should be read in conjunction with the Privacy Notice.

Definitions

In this policy the following terms have the following meanings:

'consent' means any freely given, specific, informed and unambiguous indication of an individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of persona data relating to him or her.

'data controller' means an individual or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data.

'data processor' means an individual or organisation which processes personal data on behalf of the data controller.

'personal data'* means any information relating to an individual who can be identified, such as by a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

'processing' means any operation or set of operations performed on personal data, such as collection, recording, organisation, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to an individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual.

'sensitive personal data'* means 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, data concerning health, an individual's sex life or sexual orientation and an individual's criminal convictions.

* For the purposes of this policy we use the term 'personal data' to include 'sensitive personal data' except where we specifically need to refer to sensitive personal data.

'Supervisory authority' means an independent public authority which is responsible for monitoring the application of data protection. In the UK the supervisory authority is the Information Commissioner's Office (ICO).

As an engineering service provider, Local Transport Projects Ltd processes personal data in relation to its own staff, clients and sub-contractors; and is a Data Controller for the purposes of the Data Protection Laws. The Company has registered with the ICO and its registration number is ZA059362.

The Company may hold personal data on individuals for the following purposes:

- Provide services to clients
- Advertising, marketing and public relations

- Staff administration

Data processing under the Data Protection Laws.

1. The data protection principles

The Data Protection Laws require the Company acting as either data controller or data processor to process data in accordance with the principles of data protection. These require that personal data is:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and 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;
5. Kept for no longer than is necessary for the purposes for which the personal data are processed;
6. 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; and that
7. The data controller shall be responsible for, and be able to demonstrate, compliance with the principles.

2. Legal bases for processing

The Company will only process personal data where it has a legal basis for doing so (see Annex A). Where the Company does not have a legal reason for processing personal data any processing will be a breach of the Data Protection Laws.

The Company will review the personal data it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date and those people listed in the Appendix shall be responsible for doing this.

Before transferring personal data to any third party (suppliers, customers and clients, intermediaries such as umbrella companies, persons making an enquiry or complaint and any other third party (such as software solutions providers and back office support), the Company will establish that it has a legal reason for making the transfer.

3. Privacy by design and by default

The Company has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all processing activities. This includes implementing measures such as:

- data minimisation (i.e. not keeping data for longer than is necessary)
- pseudonymisation
- anonymization
- cyber security

The Company shall provide any information relating to data processing to an individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be

provided in writing, or by other means, including, where appropriate, by electronic means. The Company may provide this information orally if requested to do so by the individual.

Rights of the individual

1. Privacy notices

Where the Company collects personal data from the individual, the Company will give the individual a privacy notice at the time when it first obtains the personal data.

Where the Company collects personal data other than from the individual directly, it will give the individual a privacy notice within a reasonable period after obtaining the personal data, but at the latest within one month. If the Company intends to disclose the personal data to a third party then the privacy notice will be issued when the personal data are first disclosed (if not issued sooner).

Where the Company intends to further process the personal data for a purpose other than that for which the data was initially collected, the Company will give the individual information on that other purpose and any relevant further information before it does the further processing.

2. Subject access requests

The individual is entitled to access their personal data on request from the data controller.

3. Rectification

The individual or another data controller at the individual's request, has the right to ask the Company to rectify any inaccurate or incomplete personal data concerning an individual.

If the Company has given the personal data to any third parties it will tell those third parties that it has received a request to rectify the personal data unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold - however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

4. Erasure

The individual or another data controller at the individual's request, has the right to ask the Company to erase an individual's personal data.

If the Company receives a request to erase it will ask the individual if s/he wants their personal data to be removed entirely or whether s/he is happy for his or her details to be kept on a list of individuals who do not want to be contacted in the future (for a specified period or otherwise). The Company cannot keep a record of individuals whose data it has erased so the individual may be contacted again by the Company should the Company come into possession of the individual's personal data at a later date.

If the Company has made the data public, it shall take reasonable steps to inform other data controllers and data processors processing the personal data to erase the personal data, taking into account available technology and the cost of implementation.

If the Company has given the personal data to any third parties it will tell those third parties that it has received a request to erase the personal data, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold - however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

5. Restriction of processing

The individual or a data controller at the individual's request, has the right to ask the Company to restrict its processing of an individual's personal data where:

- The individual challenges the accuracy of the personal data;
- The processing is unlawful and the individual opposes its erasure;
- The Company no longer needs the personal data for the purposes of the processing, but the personal data is required for the establishment, exercise or defence of legal claims; or
- The individual has objected to processing (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of the Company override those of the individual.

If the Company has given the personal data to any third parties it will tell those third parties that it has received a request to restrict the personal data, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold - however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

6. Data portability

The individual shall have the right to receive personal data concerning him or her, which he or she has provided to the Company, in a structured, commonly used and machine-readable format and have the right to transmit those data to another data controller in circumstances where:

- The processing is based on the individual's consent or a contract; and
- The processing is carried out by automated means.

Where feasible, the Company will send the personal data to a named third party on the individual's request.

7. Object to processing

The individual has the right to object to their personal data being processed based on a public interest or a legitimate interest. The individual will also be able to object to the profiling of their data based on a public interest or a legitimate interest.

The Company shall cease processing unless it has compelling legitimate grounds to continue to process the personal data which override the individual's interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

The individual has the right to object to their personal data for direct marketing.

8. Enforcement of rights

All requests regarding individual rights should be sent to the person whose details are listed in the Appendix.

The Company shall act upon any subject access request, or any request relating to rectification, erasure, restriction, data portability or objection or automated decision making processes or profiling within one month of receipt of the request. The Company may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

Where the Company considers that a request under this section is manifestly unfounded or excessive due to the request's repetitive nature the Company may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.

9. Automated decision making

The Company will not subject individuals to decisions based on automated processing that produce a legal effect or a similarly significant effect on the individual, except where the automated decision:

- Is necessary for the entering into or performance of a contract between the data controller and the individual;
- Is authorised by law; or

- The individual has given their explicit consent.

The Company will not carry out any automated decision-making or profiling using the personal data of a child.

Reporting personal data breaches

All data breaches should be referred to the persons whose details are listed in the Appendix. Data Breach Procedure can be found in Annex B.

1. Personal data breaches where the Company is the data controller:

Where the Company establishes that a personal data breach has taken place, the Company will take steps to contain and recover the breach. Where a personal data breach is likely to result in a risk to the rights and freedoms of any individual the Company will notify the ICO.

Where the personal data breach happens outside the UK, the Company shall alert the relevant supervisory authority for data breaches in the effected jurisdiction.

2. Personal data breaches where the Company is the data processor:

The Company will alert the relevant data controller as to the personal data breach as soon as they are aware of the breach.

3. Communicating personal data breaches to individuals

Where the Company has identified a personal data breach resulting in a high risk to the rights and freedoms of any individual, the Company shall tell all affected individuals without undue delay.

The Company will not be required to tell individuals about the personal data breach where:

- The Company has implemented appropriate technical and organisational protection measures to the personal data affected by the breach, in particular to make the personal data unintelligible to any person who is not authorised to access it, such as encryption.
- The Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialise.
- It would involve disproportionate effort to tell all affected individuals. Instead, the Company shall make a public communication or similar measure to tell all affected individuals.

All individuals have the following rights under the **Human Rights Act 1998** (HRA) and in dealing with personal data these should be respected at all times:

- Right to respect for private and family life (Article 8).
- Freedom of thought, belief and religion (Article 9).
- Freedom of expression (Article 10).
- Freedom of assembly and association (Article 11).
- Protection from discrimination in respect of rights and freedoms under the HRA (Article 14).

If you have a complaint or suggestion about the Company's handling of personal data then please contact the person whose details are listed in the Appendix to this policy. Alternatively, you can contact the ICO directly on 0303 123 1113 or at https://ico.org.uk/global/contact-us/email/

Appendix

People Responsible for Data control within Local Transport Projects.

Andy Mayo - Director

Annex A

a) The lawfulness of processing conditions for personal data are:

1. Consent of the individual for one or more specific purposes.
2. Processing is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual to enter into a contract.
3. Processing is necessary for compliance with a legal obligation that the controller is subject to.
4. Processing is necessary to protect the vital interests of the individual or another person.
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.
6. Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of the individual which require protection of personal data, in particular where the individual is a child.

b) The lawfulness of processing conditions for sensitive personal data are:

1. Explicit consent of the individual for one or more specified purposes, unless reliance on consent is prohibited by EU or Member State law.

2. Processing is necessary for carrying out data controller's obligations under employment, social security or social protection law, or a collective agreement, providing for appropriate safeguards for the fundamental rights and interests of the individual.

3. Processing is necessary to protect the vital interests of the individual or another individual where the individual is physically or legally incapable of giving consent.

4. In the course of its legitimate activities, processing is carried out with appropriate safeguards by a foundation, association or any other not-for-profit body, with a political, philosophical, religious or trade union aim and on condition that the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without the consent of the individual.

5. Processing relates to personal data which are manifestly made public by the individual.

6. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

7. Processing is necessary for reasons of substantial public interest on the basis of EU or Member State law which shall be proportionate to the aim pursued, respects the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the individual.

8. Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Member State law or a contract with a health professional and subject to the necessary conditions and safeguards.

9. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of EU or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the individual, in particular professional secrecy.

10. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard fundamental rights and interests of the individual.

Annex B

Data Breach Procedure

Local Transport Projects Ltd. holds some personal and sensitive data, relating to staff, clients and our suppliers. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by Local Transport Projects Ltd. and to all company staff and sub-contractors.

Purpose

This breach procedure sets out the course of action to be followed by all staff at Local Transport Projects Ltd. if a data protection breach takes place.

Legal Context

Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:
   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   (c) describe the likely consequences of the personal data breach;
   (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Types of Breach

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of staff or client data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

Managing a Data Breach

In the event that the company identifies or is notified of a personal data breach, the following steps should followed:

1. The person who discovers/receives a report of a breach must inform one of the Directors. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.
2. The Directors must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as an IT support technician.
3. As a registered Data Controller, it is the company's responsibility to take the appropriate action and conduct any investigation.
4. The Directors must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.
5. The Directors must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:
    a. Attempting to recover lost equipment.
    b. The use of back-ups to restore lost/damaged/stolen data.
    c. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
    d. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and members of staff informed.

Investigation

In most cases, the next stage would be for the Directors to fully investigate the breach. The Directors should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;

- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (clients, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Directors should, after seeking expert advice, decide whether anyone else is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the company is able to do to help them. They should also be given the opportunity to make a formal complaint if they wish (see Local Transport Projects Privacy Notice). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to mitigate the risks posed by the breach.

Review and Evaluation

Once the initial aftermath of the breach is over, the Directors should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put them right. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The Directors should ensure that staff are aware of Local Transport Projects Data Protection Policy and Privacy Notice and their requirements, including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the Data Protection Policy and associated procedures, they should discuss this with their line manager or the Directors.