Transport for London

P023 A2 Privacy and Data Protection Policy

Issue date: 1 April 2010

Effective: 1 April 2010

This supersedes any previous policy.

Purpose

1. The objective of this policy is to ensure that:

   (a) Personal Data is Processed by TfL in compliance with the requirements of data protection legislation) and other relevant information governance legislation; and

   (b) TfL Personnel are aware of their obligations when Processing Personal Data on behalf of TfL

Definitions

2. Cyber Security and Incident Response Team (CSIRT): a business unit within the Technology and Data department of Customers, Communication and Technology.

3. Data Controller: the organisation (alone, jointly or in common with other organisations) which determines the manner and purposes for which Personal Data is to be processed.

4. Data Processor: processes data on behalf of the Data Controller (other than an employee).

5. Data Protection Legislation: General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018 and any other legislation in force from time to time in the United Kingdom relating to privacy and/or the processing of personal data.. Data protection legislation governs the way in which Data Controllers such as TfL can process an individual's Personal Data. It also gives individuals certain rights regarding the information that is held about them and obliges TfL to respond to any requests from an individual to access their own Personal Data.

6. Data Protection Officer: A statutory requirement of the GDPR is the appointment of a Data Protection Officer (DPO). TfL and its subsidiaries will appoint a single DPO, reporting to a member of the Executive Committee and will ensure that the DPO is able to operate independently and is provided adequate resources to meet their GDPR obligations

7. Data Protection Principles: a set of statutory requirements, which all Data Controllers are obliged to adhere to. The Principles balance the legitimate need for organisations such as TfL to process Personal Data against the need to protect the privacy rights of the Data Subject.

8. Data Subject: an individual who is the subject of Personal Data.

9. Information Commissioner: the regulator appointed by the Crown to promote public access to official information and protect personal information. Compliance with the Data Protection Legislation is enforced by the Information Commissioner.

10. Internal Audit: a department within the Risk and Assurance function of General Counsel.

11. Personal Data: any information relating to an identifiable person who can be directly or indirectly identified by that information, in particular by reference to an identifier, including name, identification number, location data or online identifier. .Personal Data includes expressions of opinion and indications of intention, as well as factual information, and may include pseudonymised data where it is possible to attribute the pseudonym to a particular individual.

12. Personal Data Breach: the loss, destruction, damage, theft, inappropriate use or unauthorised disclosure of Personal Data.

13. Personal Information Custodians: senior managers, who are responsible for the Processing of Personal Data within their assigned area of control.

14. Privacy and Data Protection Team: a business unit within the Information Governance department of General Counsel.

15. Privacy Risk: that part of TfL's overall risk portfolio which relates to the, integrity, availability and confidentiality of Personal Data.

16. Processing/Processed: includes collecting, recording, storing, retrieving, transmitting, amending or altering, disclosing, deleting, archiving and destroying Personal Data.

17. TfL Personnel: includes all TfL employees as well as all temporary staff, contractors, consultants and any third parties with whom special arrangements (such as Data Processor, confidentiality or non-disclosure agreements) have been made.

18. Transport for London (TfL): the statutory corporation and its operating subsidiaries.

Organisational scope

19. This policy applies to all TfL Personnel and to all Personal Data Processed by or on behalf of TfL at any time, by any means and in any format.

Policy statement

20. TfL will:

(a) Comply with Data Protection Legislation and adhere to the six Data Protection Principles, as described in the Annex to this policy

(b) Comply with the statutory requirement to document its Processing of Personal Data including:

i. The name and contact details of the Data Protection Officer

ii. The purposes for which Personal Data are processed, and the legal basis for the processing

iii. Descriptions of the categories of Data Subjects and Personal Data

iv. The categories of recipients of Personal Data

v. Details of transfers of Personal Data to third countries

vi. Retention Schedules

vii. A description of the technical and organisational security measures protecting Personal Data

(c) Comply with all other relevant legal requirements which apply to its processing of Personal Data, including:

i. The Human Rights Act 1998 and the requirement to act in a way which is compatible with the right to respect for private and family life in the European Convention of Human Rights and Fundamental Freedoms

ii. The Privacy and Electronic Communications (EC Directive) Regulations 2003

iii. The common law duty of confidence

(d) Adhere to the requirements set out in the following standards, policies and guidance in order to support its compliance with Data Protection Legislation:

i. European Data Protection Board guidance on compliance with the requirements of the GDPR.

ii. The Information Commissioner's guidance documents and Codes of Practice

iii. The Payment Card Industry Data Security Standard (PCI DSS)

iv. TfL's Policy on the Disclosure of Personal Data to the Police and other Statutory Law Enforcement Agencies

v. TfL's Information and Records Management Policy

vi. TfL's Information Access Policy

vii. TfL's Information Security Policy

viii. TfL's Code of Conduct

(e) Implement appropriate structures, systems and processes to manage all Personal Data fairly and lawfully and in a way that ensures its integrity, accuracy, relevance and security

(f) Be open and transparent about how Personal Data is Processed, providing clear privacy notices at the point at which it is collected, with access to additional supporting information provided via the TfL website

(g) Consider and respond to requests from individuals who object to, or seek to restrict the Processing of their Personal Data, and consider and respond to requests to rectify or erase Personal Data

(h) Ensure that its procurement processes and contractual arrangements with external service providers include adequate measures to ensure compliance with the Data Protection Principles and associated requirements outlined in this policy, and monitor compliance with those measures

(i) Approach the identification, control, mitigation and elimination of Privacy Risk in the same way as financial and operational risk. This will be reflected in corporate and local risk registers

(j) Follow a privacy by design and default approach to ensure that Privacy and Data Protection is a key consideration in the early stages of any project, and then throughout its lifecycle

(k) Conduct a Data Protection Impact Assessment when using new technologies or planning high risk processing of Personal Data Give customers an opportunity to consent to receiving future marketing communications at the point at which their Personal Data is first collected; and within any marketing communications, provide a simple and transparent process to unsubscribe

(l) Ensure that requests from customers to change the use of their data for the purposes of marketing and/or the provision of service updates will be acted on promptly

(m) Install and use Closed Circuit Television (CCTV) and similar equipment, in accordance with the requirements of the Information Commissioner's Surveillance Camera Code of Practice and the Home Office Surveillance Camera Code of Practice

(n) Not disclose Personal Data to third parties except where disclosures are permitted by, or required by, law

(o) Label Personal Data in accordance with its Information Security Classification Standard for protectively marking Information

(p) Ensure that any complaint about TfL's processing of Personal Data or non-compliance with this policy will be passed to the Privacy and Data Protection Team. The complaint will be dealt with promptly and in accordance with TfL's Privacy and Data Protection Complaints Handling Procedure

(q) Require all TfL employees directly involved in the Processing of Personal Data to complete appropriate training on an annual basis

(r) View serious or repeated breaches of this Policy by a TfL employee as misconduct which will be managed and resolved in accordance with relevant disciplinary policies and procedures

Responsibility for privacy and data protection compliance

21. All TfL Personnel are responsible for actively supporting compliance with this policy and should only process Personal Data for legitimate business purposes directly related to the performance of their duties.

22. Personal Information Custodians are responsible for:

(a) Ensuring that TfL Personnel within their area of control are aware of this policy and are adequately trained in the handling of Personal Data

(b) The assessment and reporting of Privacy Risk linked to the Processing of Personal Data within their area of control

(c) Ensuring that Data Protection Impact Assessments are carried out Implementing and documenting appropriate procedures to ensure Processing of Personal Data within their area of control is compliant

(d) Advising the Privacy and Data Protection Team of changes in the Processing of Personal Data, in order to maintain the Data Protection documentation referred to in paragraph 20(b) above

23. The Data Protection Officer is responsible for:

(a) Providing advice and guidance on the implementation and interpretation of this Policy and/or Data Protection Legislation, including the assessment of Data Protection Impact Assessments and the provision of suitable Data Protection training

(b) Promoting, monitoring, auditing and enforcing compliance with this Policy, Data Protection Legislation and any other related statutory, common law or regulatory requirements which apply to TfL

(c) Providing a first point of contact for individuals whose data is processed, and investigating and resolving complaints about TfL's non-compliance with Data Protection Legislation and/or this Policy

(d) Liaising with the Information Commissioner's Office on any matter relating to TfL's compliance with Data Protection Legislation and/or this Policy

(e) Maintaining the documentation of TfL's processing of Personal Data

(f) Maintaining procedures for responding to a Personal Data Breach

24. All TfL Personnel are responsible for reporting actual or suspected Personal Data Breaches to CSIRT and the Privacy and Data Protection Team in accordance with the Personal Data Breach procedures

25. CSIRT is responsible for advising the business on the technical measures and controls required to protect the security and integrity of Personal Data Processed by TfL using electronic information and communications systems.

26. Internal Audit is responsible for auditing the business processes, operating procedures and working practices of TfL and its service providers which involve the Processing of Personal Data, for the purposes of monitoring compliance with this policy and alerting the Privacy and Data Protection Team to any instances of non-compliance.

Procedures/Guidelines/Processes

27. This policy will be supported by corporate instructions and guidance published via the TfL Management System.

Approval and amendments

28. This policy was first approved by the Commissioner and TfL leadership team on 22 March 2010.

29. A number of updates to the policy were approved by the Commissioner and TfL Executive Committee on 17 March 2016.

30. Further amendments to this policy to comply with the GDPR were approved by General Counsel on 23 May 2018.

31. This policy will be subject to periodic review as considered appropriate by General Counsel.

Policy owner

32. TfL's General Counsel is the designated owner of this policy.

Annex: The Data Protection Principles (General Data Protection Regulation Article 5)

Personal Data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject.

TfL will use Personal Data fairly and identify a lawful basis for processing. In any circumstance in which individuals provide TfL with their Personal Data for the first time, or if it is processed for a new purpose, they will be informed of:

- the identity and contact details of the Data Controller and Data Protection Officer;
- the purposes and lawful basis for the processing;
- any the recipients or categories of recipients of the personal data;
- the period for which the personal data will be stored;
- the rights of the individual regarding the processing of their personal data including the rights to access and data portability, rectification and erasure, restriction of processing and the right to object to processing.
- the consequences of not providing the personal data required under statute or for contractual purposes; and
- the existence of, and rights relating to, automated decision making including profiling.

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

TfL will only process Personal Data for the purpose(s) which the Data Subject was previously informed of and it will not be used for any other purpose that is incompatible with the original purpose(s). Subject to appropriate safeguards being agreed with the Privacy and Data Protection team, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

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

TfL will ensure that only the minimum Personal Data necessary for the purpose is processed and will not collect or hold Personal Data solely on the basis that it might be useful in the future. There should always be a legitimate business reason for the Processing of Personal Data linked to a specific ongoing purpose.

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

Data will be inaccurate where it is incorrect or misleading as to any matters of fact.

There must be processes in place to maintain the quality of data capture at the point data is first collected or obtained by TfL, and to accurately amend, update or correct Personal Data.

e) 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

Business areas must implement appropriate retention periods and ensure that Personal Data is securely destroyed once the purpose(s) for processing the Personal Data has come to an end; and there is no legal requirement or valid business/operational reason for its continued retention.

Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures agreed with the Privacy and Data Protection Team

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

TfL's standard contractual clauses on data protection must be used in any circumstances where Processing of Personal Data on behalf of TfL is carried out by a service provider or other third party.

The Privacy and Data Protection Team must be consulted in the early stages of any project or proposed change to a business process that has any significant implications for the Processing of Personal Data.

Personal Data will be managed in accordance with TfL's Information Security Policy.

TfL Personnel must report any actual or suspected incident, which either has or is likely to, result in the loss, theft, unauthorised disclosure, accidental destruction or other compromise of Personal Data directly to CSIRT and the Privacy and Data Protection Team in accordance with the Data Breach Procedures.

TfL will comply with the restrictions in the Data Protection Act 1998 on the transfer of Personal Data outside the European Economic Area (which consists of the member states of the European Union plus Norway, Iceland and Lichtenstein). The Privacy and Data Protection Team must be consulted in advance of any such transfers being undertaken or agreed.