Transport for London

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 the Data Protection Act 1998 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. 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.
3. Data Processor: processes data on behalf of the Data Controller (other than an employee).
4. Data Protection Act (DPA): the Data Protection Act 1998, together with all secondary legislation made under it. The DPA 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.
5. 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.
6. Data Subject: an individual who is the subject of Personal Data.
7. Human Rights Act (HRA): the Human Rights Act 1998.
8. Information Commissioner: the regulator appointed by the Crown to promote public access to official information and protect personal information. Compliance with the DPA is enforced by the Information Commissioner.
9. Information Governance: a business unit within General Counsel.
10. Information Management (IM): a business unit within Finance.

11. Information Owners: senior managers, who are responsible for the acquisition, creation, maintenance and disposal of TfL's information and Information Systems within their assigned area of control.

12. Internal Audit: a business unit within General Counsel.

13. Personal Data: information which relates to a living individual who can be directly identified from either the information itself, or by combining the information with other data available to TfL. Personal Data includes expressions of opinion and indications of intention, as well as factual information.

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

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

16. Subject Access Request: a request from an individual, under section seven of the DPA, for access to their Personal Data.

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

18. 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.

Organisational scope

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

Policy statement

20. TfL will comply with the DPA and adhere to the eight Data Protection Principles, as described in the Annex to this policy.

21. A number of criminal offences are defined in the DPA:

    (a) Knowingly or recklessly obtaining or disclosing Personal Data without the consent of the Data Controller;

    (b) Procuring the disclosure to another person of Personal Data without the consent of the Data Controller;

    (c) Repeatedly and negligently allowing Personal Data to be disclosed.

    (d) Intentionally or recklessly failing to comply with the Data Protection Principles; and

    (e) Altering, defacing, destroying or concealing data in order to prevent disclosure.

The discovery or suspicion that one of these offences may have been committed must be reported to the Privacy and Data Protection Team within Information Governance, so that they can determine whether or not the matter should be referred to the police and/or the Information Commissioner.

22. TfL will comply with the statutory requirement to maintain an accurate entry on the Information Commissioner's public register of Data Controllers which describes the purposes for which Personal Data is processed.

23. TfL will comply with other relevant legal requirements where they apply to its processing of Personal Data, including:

    (a) The HRA 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;

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

    (c) The common law duty of confidence.

24. TfL will adhere to the requirements set out in the following standards, policies and guidance in order to support its compliance with the DPA:

    (a) The Information Commissioner's suite of guidance documents and Codes of Practice;

    (b) The Payment Card Industry Data Security Standard (PCI DSS);

    (c) TfL's Policy on the Disclosure of Personal Data to the Police and other Statutory Law Enforcement Agencies;

    (d) TfL's Information and Records Management Policy;

    (e) TfL's Information Security Policy.

Policy content

25. TfL's policy is to ensure that:

    (a) It has in place structures, systems and processes to manage all Personal Data fairly and lawfully and in a way that ensures its integrity, accuracy, relevance and security;

    (b) In response to a valid Subject Access Request, TfL will tell a Data Subject whether it, or someone else on its behalf, is processing that individual's Personal Data, and if so, provide a description of: the Personal Data; the purposes for which they are being processed; and those to whom they have been, or may be, disclosed. TfL will also communicate in an intelligible form, the information which forms any such Personal Data;

    (c) TfL will respond to all Subject Access Requests within 40 calendar days of receipt of a valid request;

    (d) In response to a Subject Access Request, TfL will only refuse to provide a copy of the Personal Data which it is Processing (and any associated

information concerning its processing) if a statutory exemption applies. Any such refusal must be approved by Information Governance;

(e) Personal Data used for communicating with TfL's customers will be treated in accordance with the preferences they have expressed;

(f) Customers must be given an opportunity to opt in or out of receiving future marketing messages at the point at which their Personal Data is first collected;

(g) Requests from customers to change the use of their data for marketing purposes will be acted on promptly;

(h) Any activity intended to monitor an employee's activities in the workplace which may involve the disclosure of Personal Data or interference with the right to a private life, must be carried out in accordance with the DPA, the HRA, other relevant legislation and any duty of confidence which is owed;

(i) Closed Circuit Television (CCTV) and similar equipment will be installed and used in accordance with the Information Commissioner's CCTV Code of Practice and the Home Office Surveillance Camera Code of Practice;

(j) Personal Data will not be disclosed to third parties except where disclosures are permitted by, or required by, law;

(k) Personal Data will be labelled in accordance with TfL's Information Security Classification Standard for protectively marking Information;

(l) Procurement processes and contractual arrangements with external service providers must include adequate measures to ensure compliance with the Data Protection Principles and associated requirements outlined in this policy;

(m) Privacy Risk will be considered and afforded a priority in decisions within TfL in the same way as financial and operational risk. This will be reflected in corporate and local risk registers. Privacy Risk will be managed by a process of identifying, controlling, minimising and/or eliminating risks that may affect TfL's Processing of Personal Data;

(n) Any complaint about TfL's non-compliance with the standards set out in this Privacy and Data Protection Policy must be promptly directed to the Privacy and Data Protection Team within Information Governance. The complaint will be dealt with in accordance with TfL's Privacy and Data Protection Complaints Handling Procedure, however TfL recognises that individuals will also have the right to take their complaint directly to the Information Commissioner or, in certain circumstances (as defined in the DPA), the courts.

Responsibility for privacy and data protection compliance

26. All TfL Personnel are responsible for actively supporting compliance with this policy.

27. TfL employees involved in the Processing of Personal Data must familiarise themselves with the supporting guidance available on the TfL Management System and Intranet; and with TfL's privacy and data protection eLearning course.

28. Information Owners 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) Implementing appropriate procedures to ensure compliance with restrictions on the Processing of Personal Data within their area of control.

29. Information Governance is responsible for:

    (a) Providing advice and guidance on the implementation and interpretation of this policy;

    (b) Promoting and enforcing compliance with this policy;

    (c) Investigating and resolving complaints about TfL's non-compliance with the DPA and/or this Policy;

    (d) Liaising with the Information Commissioner's Office on any matter relating to TfL's compliance with the DPA and/or this policy;

    (e) Maintaining TfL's entries on the Information Commissioner's public register of Data Controllers.

30. Information Governance, Internal Audit and IM are responsible for managing and investigating any actual or suspected unauthorised disclosures of Personal Data and recommending measures to prevent the reoccurrence of such incidents and breaches;

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

32. Internal Audit is responsible for auditing the business processes, operating procedures and working practices of TfL and its service providers which affect the Processing of Personal Data, to monitor compliance with this policy.

Procedures/Guidelines/Processes

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

Approval and amendments

34. This policy was approved at the meeting of the TfL Leadership Team on 22 March 2010.

35. Following an organisational restructure, a number of minor amendments to this Policy were made on 2 May 2012.

36. Following a review, a number of minor amendments to this policy were approved by TfL's General Counsel on 3 October 2013.

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

Policy owner

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

Annex: The Data Protection Principles (Data Protection Act 1998, Schedule 1)

1. Personal data should be processed fairly and lawfully;

TfL will use Personal Data both fairly and lawfully. In any circumstance in which individuals provide TfL with their Personal Data for the first time, or for a new purpose, they will be informed of the identity of the Data Controller, the use to which their data will be put and whether any disclosure may be made to third parties.

This is known as a Privacy Notice and any such wording must be approved by the Privacy and Data Protection Team within Information Governance.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or 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).

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;

TfL will ensure that only the minimum Personal Data necessary for the purpose is processed and will not collect or hold data on the basis that it might be useful in the future without having a legitimate business reason for how it will be used in the present.

4. Personal data shall be accurate and, where necessary, kept up to date;

This Principle covers the integrity of Personal Data. 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 entry at the point data is first collected by TfL, and to accurately amend, update or correct Personal Data.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;

Business areas must 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.

6. Personal data shall be processed in accordance with the rights of data subjects under the DPA. These rights are to:

- Gain access to their data
- Seek compensation for substantial damage or distress caused by their data not being processed in accordance with the Act
- Prevent their data being processed in certain circumstances
- 'Opt out' of having their data used for direct marketing at any time
- Have automated decisions reconsidered.

Requests from Data Subjects to access Personal Data will be managed in accordance with TfL's Privacy and Data Protection Policy.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

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 within Information Governance must be consulted in the early stages of any project or proposed change to a business process that has implications for the Processing of Personal Data.

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

All staff must report any incident, or potential incident, likely to result in unauthorised disclosure, damage, destruction or loss of Personal Data directly to the Privacy and Data Protection Team within Information Governance.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

TfL will comply with the restrictions in the DPA on the transfer of Personal Data outside the European Economic Area. The Privacy and Data Protection Team within Information Governance must be consulted in advance of any such transfers being undertaken or agreed.