Audit and Assurance Committee

Date: **7 June 2018**

Item: **Implementation of the General Data Protection Regulation**

This paper will be considered in public

1 Summary

1.1 This paper provides the Committee with a report on implementation in TfL of the General Data Protection Regulation (GDPR) and related legislation.

2 Recommendation

2.1 **The Committee is asked to note the paper.**

3 Background

3.1 The General Data Protection Regulation (GDPR) entered into force on 25 May 2018 and, together with other legislative change introduced through a new Data Protection Act and other EU legislation still in draft (the 'e-Privacy Regulation'), will significantly affect how we use 'personal data' collected from employees, customers and other users of our services.

3.2 'Personal data' is information about any identifiable living individual, or information which enables a living individual to be identified, and includes, besides the obvious contact or biographical details, biometric information (when used to identify an individual) and identifiers such as Oyster card numbers, vehicle registration marks, IP addresses and NI numbers and data showing location or journey history or collected by CCTV, web or wifi monitoring, if it is linked, or capable of being linked, to an identifiable individual.

3.3 The proper management and protection of the personal data that TfL collects from employees, customers and others ('data subjects') is a key responsibility and an obligation TfL takes very seriously. This data is also a key resource, enabling us, for instance, to manage and recruit staff, provide customer service, operate the ticketing system and the Congestion Charge and Cycle Hire schemes and regulate the taxi and private hire trade. It is central to our plans to analyse and use data to improve our services and offers insights that can be used to increase some sources of non-fare revenue.

3.4 The changes introduced by the GDPR are evolutionary in nature but implementation has required substantial, detailed, effort to identify, review and adapt (if necessary) affected business processes and practices across many areas of TfL. The effect of the changes brought about by the GDPR is to:

(a) introduce a need to be accountable for any use we make of personal data. This involves data mapping to ensure that we know, and document in some detail, what personal data is being used, where and for what purpose. We must also identify and record the legal basis for processing such data (eg consent or the fulfilment of our statutory obligations or the performance of a contract);

(b) introduce a process to systematically identify and mitigate privacy risks, mandating the use of 'Data Protection Impact Assessments' (DPIAs) prior to any significant new use of personal data;

(c) establish the role of 'Data Protection Officer', responsible for informing and advising on our obligations to comply with the GDPR and other data protection laws and monitoring compliance, with the organisation obliged to ensure the DPO is involved in all issues which relate to the protection of personal data and has the independence and resources to carry out those tasks;

(d) increase transparency about the use we make of personal data, in the information we make available to individuals about how we use their personal data (in 'privacy notices' at the point of collection and in the Privacy pages of the website) and, more generally, through publication of DPIAs and the product of data mapping;

(e) give new or enhanced rights to data subjects to access information about themselves, to object to it being used for 'profiling', to correct that information or have it deleted (in certain circumstances) and to require that it is transferred to a third party;

(f) impose changes on our relationships with suppliers who handle personal data for us ('data processors'), who will be exposed to some liability for breaches of the Regulation;

(g) restrict the use of personal data for 'profiling' an individual's behaviour or attributes and for solely automated decision-making (even in pseudonymised form, if the individual is still linked to a persistent unique identifier);

(h) impose a mandatory reporting requirement for security breaches involving unauthorised access to or loss of personal data, within 72 hours of the incident being detected. Such incidents will have to be reported both to the Information Commissioner and, if they are exposed to significant risk as a result of the breach, to the affected individuals; and

(i) introduce a significantly enhanced enforcement regime, through a new power for the Information Commissioner to impose fines of up to four per cent of annual turnover for certain breaches of the Regulation.

4 Implementation

4.1 A GDPR Compliance Programme was established in General Counsel in 2017, under which the Privacy team is responsible for delivery of most elements of the accountability and transparency requirements, as well as training and other instructions and guidance for staff, setting broad requirements for other business areas and co-ordinating and supporting their delivery by local business areas.

4.2 Alongside this, business areas have worked to manage the impact on data, processes and systems owned by those areas, through dedicated projects in our Technology and Data and HR departments and a network of approximately sixty 'Personal Information Custodians' across TfL. Over 2,300 contracts with suppliers have also been reviewed to identify those affected by GDPR requirements, with variations being made where necessary to incorporate the specific terms and obligations required by the GDPR. Significant suppliers who process personal data for us are also undertaking their own programmes of activity to achieve GDPR compliance. A Steering Group, chaired by the General Counsel, provides governance for the Programme.

4.3 The Programme has ensured that TfL will be compliant with GDPR requirements, though a number of implementation activities are continuing. The Compliance Programme has delivered:

(a) a completed suite of new Privacy Notices to inform customers and staff how our use of their personal data complies with the GDPR. Over 250 webpages and forms have been created or amended. These have been communicated by email and letter directly to all staff and by email to 6.36m customers;

(b) an updated e-learning course 'My role in privacy and data protection' which it is mandatory for all staff handling customer or employee data to complete annually. 3,890 people completed it in the 12 months prior to 10 May 2018;

(c) updated or new instructions and guidance for staff in the TfL Management System ('Working at TfL');

(d) processes to enable individuals to submit requests to exercise the new or expanded rights they have under the GDPR;

(e) communications across the business to raise awareness, promote local action and drive completion of the e-learning course;

(f) a data mapping initiative to document, across TfL, where personal data is used, how it is managed and why it is used;

(g) new contractual clauses for use with all suppliers who handle personal data for us;

(h) a process to enable the 'Data Protection Impact Assessments' which are required for any high risk or new processing of personal data; and

(i) a process, and associated employee communications, to ensure that data breaches are reported to the Information Commissioner within the required 72 hours.

4.4 Now that the GDPR is in force, the Compliance Programme will remain in place for a further period, to drive completion of remaining activities and support on-going compliance. This will require a clear focus by business areas, taking an active and accountable role to ensure the data, processes and systems they use are compliant, and continuing active oversight and delivery by the Privacy team.

List of Background Papers:

None

List of appendices:

None

Contact Officer: Howard Carter, General Counsel
Number: 020 3054 7833
Email: howardcarter@tfl.gov.uk