Audit and Assurance Committee

Date: **6 March 2018**

Item: **Progress Report on 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 progress 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 GDPR enters into force on 25 May 2018 and, together with other legislative change being introduced through a new Data Protection Bill (expected to receive Royal Assent before 25 May) 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, 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 We have complied with the current legislation controlling the use of this data, principally the Data Protection Act (DPA) 1998, but now need to build on this to comply with the new requirements being introduced by the GDPR.

3.5 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. This is a change from the current situation, where all liability sits with us;

(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 any security breach 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;

(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.

3.6 The Data Protection Bill currently before Parliament will implement some, relatively minor, aspects of the GDPR (which otherwise has direct effect as an EU

Regulation) and also implement a separate EU Directive on the use of personal data for law enforcement purposes. This will be applicable when we are processing personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences in order to carry out a statutory function for which we have responsibility (eg when we prosecute suspected fare evaders). The Bill will repeal the current Data Protection Act.

3.7 The EU's proposed e-Privacy Regulation is intended, alongside the GDPR, to provide a new legal framework for electronic communications. Primarily aimed at providers of online and electronic communications services, it will also regulate the use of website cookies, electronic communications for marketing and the use of data generated by the interaction of consumer devices with wifi networks. A text for this Regulation may be finalised by the end of 2018.

4 Implementation

4.1 The changes introduced by the GDPR are evolutionary in nature but implementation requires substantial, detailed, effort to identify, review and adapt (if necessary) affected business processes and practices across many areas of TfL. 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 In addition to projects and local initiatives in business areas, a network of approximately sixty 'Personal Information Custodians' across TfL is also engaged, to ensure implementation is aligned with business priorities. Significant suppliers who process personal data for us are also undertaking their own programmes of activity to achieve GDPR compliance and assurance is being sought that these are adequate. A Steering Group, chaired by the General Counsel, provides governance for the Programme.

4.3 Currently the Programme is assessed as being on track to achieve compliance by 25 May, though activity will continue in a number of areas beyond that date. This reflects a self-assessment using the Information Commissioner's compliance checklist (https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/data-controllers/) and progress towards implementation of the actions identified in a recent Internal Audit report. Good progress has been made with data mapping, the identification of business processes reliant on the use of personal data, the designation of a 'Data Protection Officer', the establishment of templates and a process to carry out DPIAs, the introduction of standard GDPR compliant standard contract clauses, awareness raising, the publication of additional information on how we use personal data and the introduction of a call-off arrangement with a supplier of data breach services.

4.4 Between now and 25 May, activity will focus on the completion of:

(a) data mapping;

(b) the roll-out of GDPR-compliant contract clauses;

(c) the assessment of processes which use personal data; and

(d) the implementation of necessary process or system changes (eg to enable the fulfilment of data subjects' rights).

4.5 Further tasks include the completion of the revision of over 30 'privacy notices' and corresponding web pages, communications to inform customers of those changes, revisions to instructions and guidance for staff, and the revision of our Privacy and Data Protection Policy (and other Information Governance Policies) and relevant HR policies and terms and conditions of employment.

List of Appendices to this report:

None.

List of Background Papers:

None

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