Customer Service and Operational Performance Panel

Date: **1 November 2017**

Item: **Transparency, Freedom of Information and Data Protection**

This paper will be considered in public

1 Summary

1.1 This paper gives an update on Freedom of Information (FOI) and the development of our Transparency Strategy, and provides an overview of TfL's preparations for changes to the legislation that determines how we can use customer and employee data.

2 Recommendation

2.1 **That the Panel note the paper.**

3 Background

3.1 We published our first Transparency Strategy in October 2015 (Appendix 1) and since the Panel was updated on its implementation on 2 March 2017, we have consulted on the development of the Strategy. The consultation closed on 29 October 2017 and responses are currently being analysed.

3.2 The FOI Act and Environmental Information Regulations (EIR) require that written requests for information receive a substantive response within a statutory deadline that is usually 20 working days. TfL receives around 2,600 FOI and EIR requests a year.

3.3 The legislation governing the use of the personal data TfL collects from employees, customers and others is undergoing a fundamental, and complex, change. This will come from the implementation in 2018 of the EU's General Data Protection Regulation (GDPR), a proposed new EU e-Privacy Regulation and a proposed new UK Data Protection Act, (which is intended to implement parts of the GDPR and a separate EU Directive on the processing of personal data relating to crime and law enforcement). Some of the main changes, and their implications for TfL, are described here.

4 Transparency and FOI

4.1 The Transparency Strategy builds on our compliance with all statutory transparency requirements, such as those under the Local Government Act, the Localism Act and the Local Government Transparency Code by setting out our

presumption that all of our information should be made publicly available, unless there are legitimate reasons why not – for example, disproportionate cost, personal data or information which would harm our ability to maximise value for money for fare and tax payers.

4.2 Since the Strategy was published we have published new data on journey related sexual assault offences by taxi and private hire drivers, our gender pay gap, the status of Tram services, crowding at Tube stations, taxi rank locations, Cycle Superhighway and Quietway routes, the boundaries of the Congestion Charge and Low Emission Zones and the highway boundaries for our Road Network, Air Quality on the Underground, data on our use of Non Permanent Labour and the replies to FOI requests received since 1 January 2017.

4.3 The consultation, which closed on 29 October 2017, invited views on the objectives of our Strategy, additional datasets we should be publishing, on the format and retention period of our publications and the presentation of this material on the TfL website.

4.4 We will review the current Strategy after analysing the consultation responses and publish the updated version.

4.5 Around 230 FOI and EIR requests have been received per period in 2017/18, a 25 per cent increase on the previous year. Requests relating to taxi and private hire services have seen a particular increase. In the year to date, 91.8 per cent of all requests have been answered within the statutory deadline, which exceeds the 90 per cent performance that is expected by the Information Commissioner (who is the independent regulator for FOI, as well as the use of personal data).

4.6 The Information Commissioner monitored our performance with FOI and EIR requests received between 1 July and 30 September, as a result of a number of complaints which the Information Commissioner's Office received about overdue replies to requests made in 2016. This followed a dip in our performance in the second half of 2016. During the monitoring period we replied to over 90 per cent of all requests within the statutory deadline.

4.7 Analysis of FOI and EIR requests informs our Transparency Strategy and the identification of datasets suitable for pro-active publication. Replies to FOI and EIR requests made after 1 January 2017 are published.

5 General Data Protection Regulation and UK Data Protection Bill

5.1 The GDPR comes into effect on 25 May 2018 and is intended to provide a single legislative basis across the EU for the use of personal data in the digital economy. It applies to any organisation processing the personal data of EU citizens, no matter where the organisation is based. Personal data is a key resource for TfL, enabling us, for instance, to manage and recruit staff, operate the ticketing system and the Congestion Charge and Cycle Hire schemes and regulate the taxi and private hire trade.

5.2 The UK Government has recognised that UK businesses and public sector organisations will need to continue to comply with the GDPR after Brexit (in order for UK organisations to handle the personal data of EU citizens and for data on

UK citizens to be transferred to the EU). The Data Protection Bill is aimed at ensuring that the UK has a data protection regime in place when Brexit takes effect that provide businesses, citizens and governments with some certainty that personal data will be processed in the UK and the EU on an equivalent basis.

5.3 While many of the GDPR's main provisions and principles are consistent with the current Data Protection Act (DPA) 1998, it also introduces several new concepts, including a broadening of the definition of 'personal data', and, in general:

(a) strengthens the rights of individuals ('data subjects');
(b) increases obligations on organisations and their suppliers;
(c) places more restrictions on organisations' use of personal data; and
(d) has a significantly enhanced enforcement regime, through a new power for the Information Commissioner to impose monetary penalties of up to four per cent of annual turnover for certain breaches of the Regulation.

A summary of the GDPR is at Appendix 2.

5.4 The UK Data Protection Bill will implement those parts of the GDPR which were left to be decided by national parliaments (for instance, by proposing 13 as the age below which consent will be required from parents/guardians to process a child's personal data and setting out some of the exemptions which will apply to various provisions of the GDPR). It will also implement the Law Enforcement Directive (covering the processing of personal data for crime and law enforcement purposes) and these provisions will affect TfL's enforcement and prosecution activities and co-operation with police and law enforcement agencies.

5.5 Further legislative change will come through an e-Privacy Regulation currently being prepared by the EU. This is still in draft but it is intended, alongside the GDPR, to provide a new legal framework for electronic communications, to come into force, ideally, at the same time as the GDPR, in May 2018. 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 associated with wifi networks and consumer devices, in each case by bringing more transparency about the collection and use of personal data and giving individuals greater control over how it is used.

5.6 The GDPR's requirements will, among other things:

(a) introduce a need to document and demonstrate, if necessary on demand for the regulator, that any use we make of personal data complies with the GDPR, to satisfy its key principle of 'accountability'. This involves ensuring that we know, and 'map' in some detail, what personal data is being used, where and for what purpose. We must also identify and record the legal basis for each use of such data (for example, the performance of a contract between TfL and the data subject);

(b) 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;

(c) increase the amount of information we make available to data subjects about how we use their personal data, both in 'privacy notices' at the point of collection and in the dedicated Privacy pages of the website (this will also be a theme of the revised Transparency Strategy);

(d) affect how we identify and mitigate privacy risks, mandating the use of 'Data Protection Impact Assessments' (DPIAs) prior to any significant new use of personal data;

(e) restrict the use of personal data for 'profiling' an individual's behaviour or attributes (even in anonymised or pseudonymised form, if the individual is still linked to a persistent unique identifier). This has potentially significant implications for big data analytics associated with activities such as automated customer refunds, customer segmentation and transport planning; and

(f) 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, if the breach represents a risk to the rights and freedoms of individuals. Such incidents will have to be reported both to the Information Commissioner and also to the affected individuals, if their rights and freedoms are exposed to high risk as a result of the breach.

5.7 Complying with the GDPR is a priority for any large customer-focused, data-driven, organisation. Like banks, financial services companies, retailers, utilities, tech companies and other transport operators (eg Eurostar, Network Rail, BA), we have established a dedicated GDPR compliance programme. We have a good base to work from, having reached a relatively mature state of compliance with current legislation, and are building on this.

5.8 Work to date has included:

(a) a new project to identify contracts with current service providers which will need to be amended (up to 750 in total);

(b) changes to our procurement practices and standard contractual terms which ensure they are GDPR compliant;

(c) the identification of 'privacy notices' and supplementary information provided to customers and employees which will need to be updated;

(d) the creation of a standard DPIA template which is already being used by projects which may have a privacy impact;

(e) a programme to refresh our existing Information Sharing Protocols and Procedures with police forces and other strategic partners; and

(f) the implementation of a data breach services framework agreement with an external service provider to provide support and protection to customers or

employees affected by a data breach experienced by TfL or a supplier delivering services on our behalf.

5.9 Projects in business areas with systems and processes which are dependent on the use of personal data are reviewing changes necessary to comply with the GDPR and a procurement is underway to introduce an IT tool which will enable the use of personal data to be mapped across TfL.

6 Financial Implications

6.1 The cost of preparations for GDPR implementation is being met from existing budgets.

List of appendices to this report:

Appendix 1 – TfL Transparency Strategy (2015)
Appendix 2 – GDPR Summary

List of Background Papers:

None

Contact Officer: Howard Carter, General Counsel
Number: 020 3054 7832
Email: howardcarter@tfl.gov.uk

Appendix 1

Transport for London – Transparency Strategy

October 2015

Transport for London – Transparency Strategy

Introduction

Transport for London - our purpose

We are London's integrated transport authority, responsible for implementing the Mayor's Transport Strategy. Our purpose is to keep London working and growing and to make life in the Capital better.

We are funded by income from fares, revenue raised from fees and charges, commercial property and advertising, borrowing and Government grants. Every penny of our income is reinvested in running and improving transport to ensure that London remains a world-leading city.

Our services

We are responsible for London Underground, London Buses, Docklands Light Railway, London Overground, London Tramlink, London River Services, Dial-a-Ride, Victoria Coach Station, Santander Cycles and the Emirates Air Line.

We regulate taxis and the private hire trade, operate the Congestion Charging scheme, manage the 580km red route network of London's key strategic roads, and operate 6,000 traffic signals.

We work with many partners to improve life in London. This includes taking action on road safety and enabling people to make sustainable travel choices, such as cycling and walking.

We are also delivering one of Europe's biggest programmes of capital investment, including building Crossrail, modernising the Tube and road networks and delivering the Mayor's vision for cycling.

We are determined to operate in an open and transparent way, for the benefit of our customers, stakeholders and those who hold us to account.

We recognise that with responsibility for billions of road and public transport journeys every year and an annual budget of around £11bn, we have a duty to spend that money as efficiently as possible and account for every penny.

We publish a huge amount of data reflecting the scale of what we do including contracts, expenditure, operational and financial performance, customer satisfaction and journey patterns. This helps us to explain how we run London's transport network and plan for its future. We now publish more information on how we operate than ever before. Much of this is designed to explain how we reinvest public money to improve transport for customers and road users. Our dedicated 'Transparency' and 'Publications and Reports' sections on our website show where this information can be obtained.

Openness and transparency in these and other areas is helping to transform the way in which we operate. It helps our customers use our services more effectively,

strengthens our relationships with customers and stakeholders, and helps us to work with local communities and businesses to improve our services.

Our provision of free real-time open data also enables innovation in the way our customers travel. Hundreds of smartphone apps developed by third parties are being powered by our data.

Our approach to transparency

We are committed to operating in an open and transparent way and fully recognise the benefits this offers our customers, stakeholders and, of course, us.

By being open and accountable we:

- Enable our customers and stakeholders to hold us to account, contributing to better decision-making and enabling public input into those decisions
- Deliver better value for money
- Engage businesses, non-profit organisations, academics and others to make transport in London better

We publish all the documents required by statute and supplement these to publish a range of documents which provide a detailed insight into our priorities, targets and delivery:

- Business Plan – our 10 year plan of investment and operational improvements and the financial resources required for their delivery
- Annual Budget – how the 'first' year of the Business Plan will be delivered, including that year's detailed budget and performance targets
- Annual Report and Statement of Accounts – overall performance in the previous financial year including investment and operational performance, remuneration and statutory accounts
- Operational and Financial Performance Report – quarterly reporting setting out performance against annual budget
- Investment Programme Report – quarterly reporting on progress of the investment programme against annual budget and milestones
- Commissioner's report to the Board – the main highlights of all TfL's activities and performance since the previous Board meeting
- Annual report for Health, Safety and Environment – to provide our stakeholders with additional information on these core areas of our business

We constantly analyse what our customers and users tell us is important to them. We gathered views through a public consultation on our approach to transparency and routinely analyse, among other sources, questions and complaints, regular customer research, scrutiny by the London Assembly and London TravelWatch and Freedom of Information requests.

This analysis allows us to identify core areas of public interest and thus the new data sets which we should publish as a matter of course rather than waiting to be asked for them.

Our published information is focused on:

- Our operational performance, including the reliability and safety of public transport and the road network, and data on ticketing derived from the Oyster and contactless payment card system
- Progress on delivery of our investment programme which is modernising public transport and roads infrastructure
- Our people, including levels of remuneration and expenses
- Real-time customer information on the status of public transport and roads, including open data feeds that can be used by third parties free of charge
- Overall value for money, including commercial contracts and sponsorships

Operational performance

We must ensure that millions of journeys are made safely and reliably every day and publish data on our operational performance, through the Operational and Financial Report to the Board. Additional examples of more detailed information published about our operations are:

- Detailed and frequent performance information published on our website in the 'Transparency' and 'Publication and reports' sections
- Information on planned modernisation work which might disrupt journeys, including sending information out each week to millions of customers and users who have registered to receive service-related emails from us
- An array of live 'service status' information
- Crime figures on public transport
- Data on all road collisions, including the number of people killed and seriously injured
- Data on all collisions involving buses under contract to TfL
- A range of operational information derived from the Oyster and contactless payment card system
- Bus-related crime data by borough, based on figures provided by the Metropolitan Police Service
- Bus operator league tables, showing performance against a number of measures
- The performance of TfL Customer Services

In addition, we publish more general information on our operations, such as customer research and guidance on how to get the best out of the services we operate. We help customers to understand the features of Oyster and contactless payments and how they can make sure they pay the right fare and get the best value for money.

This includes promotion of daily and weekly fare capping, off-peak fares, remembering to touch in and out, and refunds following service delays.

The investment programme

Increasing capacity and connectivity is central to meeting the needs of a rapidly expanding world city. London is growing faster than anyone expected a few years ago, with its population expected to rise from 8.6 million today to around 10 million by 2030. To accommodate this, we must increase services and unlock areas of economic development. This requires better local connections, more people using sustainable transport and the capacity to take people to where they work.

Our quarterly Investment Programme Report to the TfL Board describes our major programmes and projects designed to expand capacity. It describes the objectives of each, the financial cost and their progress against milestones. We also publish:

- Details of our most significant projects, including through short films, available via our website
- An annual report, which sets out the improvements we have delivered

Our people

We publish:

- A high-level organisation chart, with contact details
- Extensive details of the remuneration of staff
- Our annual Workforce and Monitoring Report and Single Equalities Scheme describing the composition of our workforce
- Biographies of all Board members and Chief Officers, with declarations of interests, a register of gifts and hospitality and any expenses claimed

Customer information

We reinvest all of our income into running and improving our services. Explaining this is a common theme in our public communications, helping to set out how we use public money to benefit the economy of London and the UK.

Customers rightly regard real-time travel information as part of the core service we provide. Their expectations of how they should be kept informed and how they transact with us have shifted dramatically, and will continue to do so.

Examples of how we have adapted to these expectations include:

- Providing a real-time commentary on the status of transport services via our website and social media such as Twitter
- Films on our website that answer customers' most frequently asked questions in an accessible way
- Factsheets to help customers get the most from our services and make sure any charges, such as the Congestion Charge, are fully explained

- Complaints levels, the major themes which emerge from complaints and the action we take to address them
- All live feeds of operational service status are made openly and freely available in machine readable form

Thousands of developers and others use our feeds to create real-time travel information apps for millions of customers. The Shakespeare Review, commissioned by the Government in 2013 to consider the use of open data created by the public sector, noted that this approach benefited our customers by up to £58m each year in time saved.

We are proactive in explaining to our customers how we will handle personal information that they share with us. This includes publishing detail on what we do with their data, who it is shared with and how long it is retained.

Value for money

Delivering value for fare and tax payers' money is central to everything we do. We explain how we spend public money productively and the resulting benefits through publishing:

- Details about our financial decision making, including agendas, papers and minutes from Board and other key governance meetings
- Details of all expenditure over £250
- Details of all contracts worth more than £5,000 and any that have been released as a result of a Freedom of Information (FOI) request
- All contracts announced in a press release, as well as those concluded as a result of an invitation to tender issued after 1 September 2013, where the value of the contract exceeds the applicable OJEU threshold. This includes revenue raising contracts (such as deals for sponsorship or property development) as well as contracts for the purchase of goods and services
- Contract opportunities
- Internal audit reports, showing the actions we have taken

In addition, we communicate any discounts customers might be eligible for by promoting Zip Oyster cards for children and adult discount and concession cards. This includes supporting London Councils to promote Freedom passes.

Accountability

We have substantially changed the way information is made available about our decision-making. We have published the information required by the Government's 2015 Local Government Transparency Code and met all of the requirements in relation to disclosure of remuneration data.

We answer around 2,500 FOI requests a year, providing access to an even greater range of data, often of particular benefit to individuals with a local or specialist interest in our operations.

We also use these requests to identify information that we should publish routinely, such as London Underground's working timetables or data on the use of Oyster and contactless payment cards. In 2014/15 84 per cent of all FOI requests resulted in the disclosure of information in full and 87 per cent of all FOI requests were answered within statutory deadlines.

Approximately 2,000 questions put to the Mayor by the London Assembly about TfL through the Mayoral Question Time process are also answered each year, as well as around 2,500 pieces of correspondence from Assembly Members.

Our commitment to transparency

Our presumption is that all our information should be made publicly available and, in the case of data, provided in machine readable form, unless there are legitimate reasons why not – for example, disproportionate cost, personal data or information which would harm our ability to maximise value for money for customers and tax payers.

All the information we publish is available through our website and we will ensure that it is easily identifiable (including via improved search), accurate and up-to-date and, where appropriate, available in machine-readable form.

We will normally make data available on our website for as long as is necessary to ensure accountability and establish trends. We assign staff to own our published information and take responsibility for its quality.

We align with the Principles set out by the Government's Public Sector Transparency Board and where our practice differs (eg on the use of data.gov.uk or in the requirement for app developers to register with us to gain access to our data feeds) we consider that this brings benefits to the users of our data.

We will develop and publish a schedule which outlines when we plan to make specific information available such as publications, Board papers, replies to FOI requests and datasets. This will initially cover regular publications and will expand to include ad hoc and planned future information as far as is practicable.

Further developing our approach

We will formally review our overall approach to transparency on an annual basis and keep stakeholders informed and involved in its development. We aim to continuously develop the range and quality of information we make available. Twice a year we will publish an update summarising developments in this area, and comments on our approach are welcome. These can be sent to HowardCarter@tfl.gov.uk or VernonEveritt@tfL.gov.uk.

Appendix 2

Area	Countdown to 2018	Extra-territorial reach	Core rules remain the same	Consent	Data subjects' rights	Accountability	Privacy notices	Data protection officers	Data security	Processors	Transfers outside the Union	Sanctions
Summary of Regulation	> The GDPR will apply in all Member States from 25 May 2018. > Businesses that carry out crossborder processing should be primarily subject to the regulator in the jurisdiction in which they have their main establishment.	> The GDPR primarily applies to businesses established in the EU. > It will also apply to businesses based outside the EU that offer goods and services to, or monitor individuals in, the EU.	> The GDPR retains the same core rules as the existing Data Protection Directive but there are some significant changes to those rules. > The concept of sensitive personal data has been retained and expanded to include genetic and biometric data. Using information about criminal offences will also be harder to justify.	> It will be much harder for you to obtain a valid consent under the GDPR. Individuals can also withdraw consent at any time. > Consent to process sensitive personal data or to transfer personal data outside the EU must be explicit. > However, you will not always need consent. There are other justifications.	> There are also potentially significant new rights for individuals, including the "right to be forgotten" and the right to data portability. > The new rights are complex and it is not clear how they will operate in practice.	> Under the GDPR, you must not only comply but also be able to demonstrate you comply. > If you are carrying out "high risk" processing, you must carry out a privacy impact assessment and, in some cases, consult your regulator. This could have significant timing implications for your project.	> The GDPR increases the amount of information you need to include in your privacy notices. > Those notices must also be concise and intelligible.	> You may be obliged to appoint a data protection officer. > The data protection officer must be involved in all data protection issues and must report directly to the highest level of management within your organisation.	> You must keep personal data secure. This obligation is expressed in general terms but does indicate that some enhanced measures, such as encryption, may be needed. > You may have to report security breaches to the regulator and, in some cases, to individuals.	> You will need to include new obligations in contracts with your data processors. > Some aspects of the GDPR are directly applicable to processors. This will be a major change for some suppliers who were previously not subject to data protection law.	> The GDPR prohibits the transfer of personal data outside the EU, unless certain conditions are met. These conditions are broadly the same as those under the existing Data Protection Directive. > Full compliance with these rules will continue to be difficult and requests from foreign regulators will be challenging.	> There is a step change in sanctions. Regulators will be able to issue fines of up to 4% of annual worldwide turnover or €20 million. > Individuals can sue you for compensation to recover both material damage and non-material damage (e.g. distress).
"To do" list	☑ Work out where your main establishment is and who your lead regulator will be. ☑ Keep track of guidance issued by regulators and the European Data Protection Board.	☑ Evaluate if your business (if established outside the EU) is nonetheless caught by the GDPR. If you are caught, you may need to appoint an EU representative. ☑ Consider if you want to take steps to avoid being subject to the GDPR.	☑ Review your existing compliance. ☑ Work out if you are processing genetic or biometric information or information about criminal offences. If so, bring that processing into line with the new requirements of the GDPR.	☑ Review your existing processes to obtain consent to determine if they are valid under the GDPR. ☑ Consider if you can rely on an alternative basis for processing, especially in light of the right to withdraw consent.	☑ Consider if individuals are likely to exercise their new rights against you and what they mean for your business in practice. ☑ Based on that analysis, set up processes to capture, record and act on those requests.	☑ You will need to create and maintain a record of the processing you are carrying out (unless exempt). ☑ You should adapt your product development processes to include a privacy impact assessment.	☑ You will have to update your existing privacy notices. ☑ You should use the most effective way to inform individuals of your processing, such as layered or just-in-time notices.	☑ Work out if you need to appoint a data protection officer or want to appoint one on a voluntary basis. ☑ Consider if you want to appoint a single data protection officer for the whole of your business.	☑ Consider setting up a central breach management unit to collate, review and notify breaches, where appropriate. ☑ Review and update your security measures in light of the increased security obligations in the GDPR.	☑ If you are a controller, update your contracts with processors to reflect the new contract requirements. ☑ If you are a processor, consider the implications of becoming directly subject to the GDPR.	☑ Review your current transfers and consider if they are justified now and will continue to be justified under the GDPR. ☑ You should consider implementing a "structural" transfer solution (such as Binding corporate rules or an intragroup agreement) to justify your transfers.	☑ Review your current level of compliance and bring it up to the level required under the GDPR. ☑ Consider your overall attitude to risk and consider creating a risk assessment framework.