The General Data Protection Regulation

An introduction to the new law and how it will affect TfL

EVERY JOURNEY MATTERS

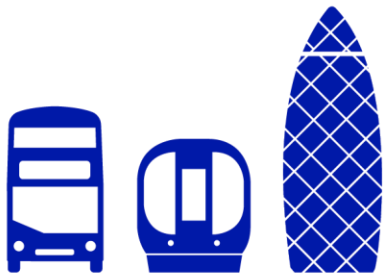
The General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a new piece of legislation which was adopted in May 2016 by the institutions and Member States of the European Union (EU). It will come into force on 25 May 2018, replacing most of the provisions of the UK's Data Protection Act 1998 (DPA) and other local data protection laws across the EU. Among other changes, it will introduce tougher rules on how personal information must be handled and protected, and much higher financial penalties for non-compliance. It's important to note that some things don't change under the new law:

- the GDPR includes the same key principles as the DPA and regulates the processing of all forms of personal information
- organisations processing personal data do so as either a data controller (eg TfL) or a data processor (eg an external service provider like Cubic, Serco, ITAL or Capita). A data processor can only process personal information in accordance with the instructions of the data controller; and an appropriate data processor agreement must be in place
- all processing of personal information must comply with a set of general principles and be carried out for a legitimate purpose
- the concept of 'sensitive personal data' has been retained and expanded to include genetic and biometric data

The Privacy and Data Protection Team are currently assessing the impact of the GDPR on TfL, its operating subsidiaries and service providers. However, it's already clear that a significant number of business processes and supplier agreements involving the processing of personal information will need to be modified. The TfL Directorates likely to be most affected by the GDPR are listed below:

- Customer Experience
- Commercial



- Commercial Development
- Enforcement and On-Street Operations
- Human Resources
- Marketing
- Surface Service Operations

After reviewing the contents of this briefing note (which will tell you more about some of the key changes being introduced by the GDPR), if you have any questions or concerns about how the GDPR may affect your business area, please contact the Privacy and Data Protection Team.

What happens when the UK leaves the EU?

The UK will remain a full member of the EU until the terms of its withdrawal have been finalised. That process is unlikely to have been completed before May 2018 when the GDPR comes into force. This means that there is no immediate impact on either existing UK privacy and data protection law or the planned implementation of the GDPR.

Both the Information Commissioner's Office (the UK regulatory authority which enforces privacy and data protection legislation) and the UK Government have made clear that organisations based in the UK should continue to plan for the full implementation of the GDPR.

Whatever the eventual outcome of the Brexit negotiations, it's unlikely that the UK will adopt a weaker set of rules on data protection. In the recent past, other countries (for example, Canada, New Zealand, Japan and Australia) have implemented very similar data protection laws to the EU, partly to facilitate cross-border exchanges of personal information.

Privacy notices

The GDPR will mean that we have to provide some additional information in our privacy notices. TfL already takes an open and transparent approach to how we collect and process personal information, as can be seen from the Privacy & Cookies section of the TfL website, but some changes may still need to be made.

Organisations will have to use the most effective way to inform individuals about how their personal information will be processed, for TfL this will generally mean a 'layered' privacy notice (ie a short paragraph of text on a web form, or in a pop-up text box in an app, which includes a link to a more detailed explanation on a dedicated web page).

A process is underway to review all of TfL's existing privacy notices.

Consent

Obtaining an individual's consent is one way for TfL to ensure that it is processing their personal information in accordance with data protection law (although there are also other ways to do this). However, it will be harder for TfL to obtain a valid consent under the GDPR and individuals will find it much easier to withdraw that consent at a time of their choosing.

As under the DPA, consent to process sensitive personal data (eg about their health, ethnicity or past criminal convictions) must be clear and explicit. Consent to transfer personal information outside of the European Economic Area will now also need to be explicit.

A process is underway to review the ways in which TfL obtains consent to process personal information and determine if they will remain valid under the GDPR. In some cases we may be able to rely on an alternative basis for processing personal information and this helps to address the problems which may arise as a result of the right of individuals to withdraw their consent.

Where TfL does continue to rely on an individual's consent as a basis for processing their personal information, relevant business areas will need to put in place processes for recording (and acting on a withdrawal of) that consent.

Children

Consent from a child, in relation to any online services provided by TfL, will only be valid if it is authorised by a parent or guardian. A child is someone under 16 years old, though the UK and other EU Member States can choose to reduce this age to 13 years old.

The GDPR contains some other provisions affecting children, for example:

- privacy policies and privacy notices must be clear and easy to understand if they are aimed at children
- profiling and automated decision making should not be applied to children; and
- the 'right to be forgotten' (ie for personal information to be deleted or de-personalised) applies very strongly to children

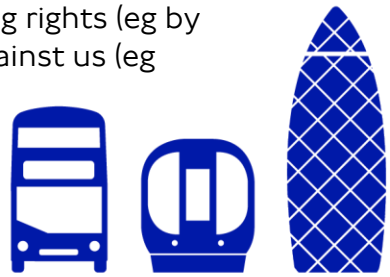
A process is underway to review all of TfL's business processes that involve the processing of personal information relating to children (including our concessionary travel schemes), to assess whether any changes need to be made as a result of the GDPR.

Data subject's rights

The GDPR retains the existing rights of individuals to access their own personal data; correct inaccurate data; challenge automated decisions made about them; and object to direct marketing.

There are also some new rights for individuals, including the 'right to be forgotten' (ie for personal information to be deleted or de-personalised) and the right to 'data portability' (ie for personal information to be extracted and given to another data controller at the data subject's request).

A process is underway to review the way in which TfL responds to individuals who choose to exercise their existing rights (eg by submitting a Subject Access Request) and assess how likely it is individuals will want to exercise any new rights against us (eg to ask for their Oyster journey history to be deleted). Based on that analysis, some business areas may need to set up new processes to capture, record and act on those requests.



Accountability and evidence of compliance

Under the GDPR, TfL not only has to comply with the six general principles and associated rules on the processing of personal information; it must be able to demonstrate that we are complying with them.

If TfL is planning to process personal information in new or different ways, business areas already have to carry out a Data Protection Impact Assessment (DPIA). As a result of the GDPR this will become a legal obligation as well as a TfL policy requirement, and in some cases the Privacy and Data Protection Team may also have to consult the Information Commissioner's Office before TfL can start processing the personal data in question. This could have implications for project timescales and resourcing requirements.

A process is underway to review TfL's Privacy and Data Protection Policy to ensure that it requires business areas to keep appropriate records of the ways in which they are processing personal information. Based on that analysis, some changes may need to be introduced, for example a requirement for business areas to complete an annual online questionnaire which would capture the details of any processing of personal information.

External service providers acting as data processors

The GDPR expands the range of provisions that TfL must include in their contracts with data processors (ie external service providers who will be processing personal information on behalf of TfL.

A number of the requirements in the GDPR will apply directly to TfL's data processors (eg they will become jointly liable for compensation claims by individuals which relate to the processing of their personal information). This is a major change for some service providers and it could have a significant commercial impact (ie with some, or all, of any associated costs being passed on to data controllers).

A process is underway to update TfL's standard privacy and data protection contract clauses as well as the guidance available at Working with external service providers. The Privacy and Data Protection Team will also be working closely with colleagues in Commercial to update data processor terms and conditions in existing agreements with external service providers.

Offshore processing

The GDPR prohibits the transfer of personal data outside the European Economic Area (EEA), unless special conditions are met. Those conditions are designed to ensure an adequate level of protection for the personal information being transferred and processed outside the EEA and are broadly the same as under the DPA.

A process is underway to review the processing of personal information carried out on behalf of TfL in countries outside of the EEA (which is made up of the EU Member States plus Norway, Iceland and Lichtenstein) and assess whether they are protected by adequate safeguards and can therefore continue beyond May 2018 (when the GDPR comes into force).

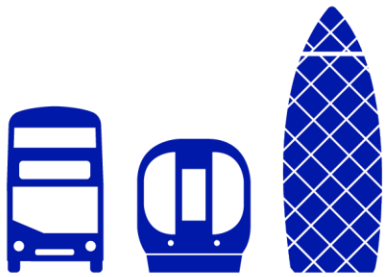
Security of personal information

The GDPR imposes a duty on data controllers such as TfL, to keep personal information secure. This obligation is expressed in general terms, but does make clear that some enhanced measures, such as encryption, may be needed depending on the sensitivity of the personal information concerned.

TfL will have to report any serious personal information breaches to the Information Commissioner's Office, normally within 72 hours. We may also have to tell affected individuals.

A process is underway to review TfL's Information Security Policy and Information Security Classification Standard to ensure that they address all of the requirements contained in the GDPR.

Colleagues in the Cyber Security and Incident Response Team (CSIRT) have developed a number of new cyber security policies and a comprehensive incident management process, which will apply to any information security breaches involving personal information processed by TfL or its external service providers.



Sanctions and enforcement

Under the GDPR there is a big increase in the maximum fines that the Information Commissioner's Office can impose on a data controller who breaks the law (under the DPA the maximum fine that can be imposed on a data controller is currently £500,000). The GDPR creates two levels of maximum fine.

The first is up to 4% of annual turnover (for TfL this would be roughly £400,000,000); and it applies in the following situations:

- failure to comply with the general principles which apply to the processing of personal information (ie it must be legal, fair, limited, secure and based on consent, performance of a contract, or the protection of vital interests)
- processing sensitive personal data (ie racial or ethnic origin, sexual life, political opinions, religious beliefs, trade union membership, genetic or biometric data) in a non-compliant way
- breaching the rights of data subjects (including their rights to: access their personal information; have inaccurate information corrected; be forgotten; object to how their information is being processed)
- transferring personal information to countries which do not provide adequate protection and safeguards for personal information

The second is up to 2% of annual turnover (for TfL this would be roughly £200,000,000) and it applies in the following situations:

- appropriate consent is not received from children
- security measures are inadequate
- failure to notify a personal data breach
- a controller uses a processor who does not comply with the GDPR
- record keeping does not meet the new GDPR requirements

- Failure to co-operate with the Information Commissioner's Office

- failure to conduct a Data Protection Impact Assessment (DPIA) where the processing is likely to result in a high risk to the rights and freedoms of individuals

The Information Commissioner's Office will still have a wide range of other powers they could choose to use against TfL if they believe we are not complying with the GDPR or other privacy and data protection legislation. They could audit us, issue formal warnings and/or issue either a temporary or permanent ban on the processing of certain types of personal information.

Individual data subjects will also be able to take legal action against TfL to try and recover damages for financial losses and/or any distress they have suffered as a result of how TfL has processed their personal information.

Further information

The Privacy and Data Protection Team will be providing advice and guidance to those business areas most likely to be affected by the GDPR. Additional information will also be published on the Managing personal information section of the TfL Management System over the coming months.

In the meantime, The Information Commissioner's Office has published some general guidance for UK data controllers which may be of interest:

- The General Data Protection Regulation: 12 steps to take now

- Overview of the General Data Protection Regulation

Contact

Privacy and Data Protection Team
Transport for London
Windsor House
42-50 Victoria Street
London SWIH 0TL

Email privacy@tfl.gov.uk

TfL website tfl.gov.uk/privacy