

GDPR Compliance Programme: Key work streams and activities

Personal data mapping

A personal data mapping exercise will need to be carried out to capture and document the processing of personal data across every area of the TfL group (ie TfL and its subsidiaries) and its key data processors. This exercise forms a vital element of the new record keeping and accountability obligations contained in the GDPR. Some of the key questions which will be directed to business areas as part of the personal data mapping process, are summarised below:

- what personal data is being collected?
- how is that personal data being collected?
- why is that personal data being collected?
- which business area (and/or legal entity) is collecting it?
- which Personal Information Custodian is responsible for that personal data?
- where is that personal data being stored?
- how is that personal data being used?
- how is that personal data being secured?
- who has access to that personal data?
- who is that personal data being shared with?
- how long it is that personal data being retained?
- how is it that personal data being deleted/destroyed?

The scale of this task means that an external service provider may be best placed to carry out the associated surveys, interviews and site visits.

Gap analysis and remediation

Following the completion of the personal data mapping exercise it is likely that a significant number of remedial actions are identified to bring TfL systems and business processes into compliance with the requirements of GDPR. Where possible these will need to be co-ordinated by the relevant business area, however, they will need to be tracked and monitored centrally as part of the wider GDPR Compliance Programme.

Annual Data Protection Compliance Assessments

A new rolling programme of annual Data Protection Compliance Assessments needs to be established across TfL and its key data processors. This will take the form of an annual return (in the form of a questionnaire) to be completed and submitted online (by TfL business areas or service providers) using the [TRUSTe Assessment Manager](#) privacy



assurance tool (which will also be used for the completion of Data Protection Impact assessments).

Risk management

To support the identification and mitigation of privacy and data protection risks across the business a new risk category will need to be created within ARM ([Active risk Manager](#)). Appropriate guidance will also need to be issued to the business to support the identification of relevant risks and ensure that they are captured either within ARM or on local risk registers.

Awareness campaigns

A general internal awareness campaign needs to be planned and implemented with the assistance of Employee Communications & Engagement. Ideally this will include: news articles on Source, the LU Intranet, OTM, Upfront and other publications; an animated film for use online and in presentations and briefings; posters and flyers for operational staff at LU stations and depots, bus stations and Dial-a-Ride depots.

Additional, more targeted, awareness campaigns are also likely to be required in the context of individual work streams (eg annual DP Compliance Assessments, privacy risk management, etc).

Data processor contract variations

Between 400 and 700 data processor agreements with external service providers may need to be amended to incorporate [revised privacy and data protection contract terms and conditions](#) (which have already been completed). This process will involve a “letter of variation” containing the new clauses, being sent to the service providers. They will need to sign and return the letter to confirm acceptance; however some service providers are likely to want to negotiate some amendments to the proposed clauses.

The letters are likely to be issued by Commercial between June 2017 and February 2018 (in three batches based on high, medium and low risk/priority) and TfL Legal will be assisting the PDPT with the drafting of the template letters of variation.

Privacy notices and web pages updates

TfL currently uses more than 30 different Privacy Notices which are presented to data subjects at the point where their personal information is collected. These are supported by a series of seventeen [online privacy pages](#) published on the TfL website. All of this content will need to be reviewed and assessed against the relevant requirements contained in the GDPR. New online privacy pages will also need to be created on topics such as TfL apps and TfL’s use of social media.

Privacy and Data Protection Policy update

The [Privacy and Data Protection Policy](#) will need to be reviewed and assessed against the requirements of the GDPR and any associated guidance issued by the Information

Commissioner's Office. Any amendments will need to be approved by the Commissioner and ExComm.

Updates to the TfL Management System

Content within the [TfL Management System](#) will need to be reviewed and assessed against the requirements of the GDPR and any associated guidance issued by the Information Commissioner's Office. It's likely that new content will also need to be created on the TfL Intranet (in cases where guidance falls outside the scope of a "work instruction").

Updates to Information Sharing Protocols and Procedures

TfL currently has 10 [Information Sharing Protocols](#) and around 20 associated Information Sharing Procedures governing the sharing/transfer of personal data with other public authorities. A revised GDPR compliant template for these agreements has already been produced, but all existing agreements need to be amended so that they are consistent with that new version. This process is likely to involve some negotiation with partner organisations.

A series of new Information Sharing Procedures (under the existing Information Sharing Protocols) also need to be drafted and signed, ideally in advance of May 2018.

Update to Subject Access Request forms/processes

TfL currently has approximately 11 [Subject Access Request forms/processes](#) which allow data subjects to seek access their personal data in accordance with the law. All of these which will need to be reviewed and assessed against the requirements of the GDPR and any associated guidance issued by the Information Commissioner's Office.

eLearning update

Existing eLearning content within the mandatory "[My role in privacy and data protection](#)" course will need to be reviewed and assessed against the requirements of the GDPR and any associated guidance issued by the Information Commissioner's Office. Additional eLearning modules may need to be developed for specific topics, eg de-personalisation/anonymisation of data; processing personal data associated with children; etc).