Transport for London's approach to data ethics

Every day, hundreds of thousands of people travel across London using Transport for London (TfL) services, with every journey leaving a trail of data that helps TfL understand its users and improve its offer to the public.

At TfL, data ethics and data privacy go hand in hand. They are considered at the same time as part of a broad approach to thinking about the impact their data decisions have on the public and on society. This approach is reinforced by Lauren Sager Weinstein, Chief Data Officer at Transport for London, who says: "Trust is our licence to operate."

When TfL starts a new initiative, or makes a significant change to an existing process involving personal data, it will carry out a Data Privacy Impact Assessment (DPIA). Examples of this include the data from customer journeys and tapping in and out of the network with an Oyster card, or how TfL kept people safe from Covid during the pandemic,

TfL has mirrored the Open Data Institute's Data Ethics Canvas in its DPIA process. Each of the 15 elements of the Canvas are reflected in the DPIA so that privacy and ethics are as one. From identifying the need for data, how it will be found and accessed through to engagement and consideration of impact and risk, the process is robust and challenging.

Considerations of data privacy are part of how projects are managed by TfL, with the creation of a DPIA critical to a project successfully passing its first gateway and ensuring it proceeds through to project delivery. A DPIA may have been through many iterations along the way.

The Data Privacy and Data Protection team are a professionalised service in TfL and offer support to those needing to carry out the assessments; the leader of this team will ultimately sign off the DPIA. There are regular meetings of the leader of this team, along with leaders in information governance, privacy advisers and the Chief Data Officer. They offer challenge and peer review and assurance that due process has been followed.

Responsibility for review of the DPIA, and for updating it to avoid function creep, will generally sit with the data owner. The Data Privacy and Data Protection team will revisit and update the DPIA if there are changes to processes or objectives, or if new risks or mitigations are identified.

A recent Covid-related example of a completed DPIA can be found [here](#).

October 2021