Transport for London:

Response to MoJ Call for Evidence on the European Commission's data protection proposals

1. Conditions for consent and the impact of changes to conditions for lawful processing

We have concerns about the statement that consent will be invalid where the relationship is considered to involve a significant imbalance between the parties involved – and the ability for consent to be refused or withdrawn without detriment.

In the context of being a provider of transport services, this could restrict the provision of our products or services. For example, access to some products or services are only offered on the basis that the individual provides certain personal information about themselves.

For example, 'Dial-a-Ride' services for individuals with mobility issues are only available to individuals who can demonstrate their eligibility and therefore benefit from the service (the information required in this case is health related). If the relationship between TfL and the customer is deemed to be imbalanced here and consent not considered to be freely given, it is difficult to see how TfL could legitimately process these individuals' data.

In addition, some TfL products and services are only available to customers who register and agree to provide some personal data. Those who choose not to consent or provide this data are limited in their access to say, online customer services (because we cannot verify who they are) or are unable to load certain higher value ticketing products onto their Oyster card. Under the revised legislative framework might these customers potentially be viewed as suffering a detriment?

Additionally, the condition for processing found in Art 6(1)(f) – relating to processing for the legitimate interest of the data controller, will not be available to public authorities. This represents the withdrawal of a very important gateway to legitimate processing for many public authorities who may find it difficult to rely on any other condition to make their processing lawful.

When taken in conjunction with the inability to rely on consent as a gateway to lawful processing, this will severely restrict TfL's ability to legitimately process personal data and continue to offer the range of products and services which we currently make available.

2. Subject Access Requests

It is of great concern that the time period for a response is likely to be reduced from forty days to one month. It is also a concern that the ICO in its initial analysis goes further and recommends an even shorter period in respect of electronic information (it is wholly incorrect in its assertion that electronic information is easy to retrieve and disclose when most data controllers operate many different databases, applications and systems which may not be integrated for the purposes of ediscovery).

TfL is a large organisation with over 23,000 employees and many millions of customers. It receives a large volume of complex subject access requests and meeting this requirement would result in significant cost to the business as we would need to invest in additional employees and technologies dedicated solely to the location, retrieval and evaluation of personal data prior to disclosure.

The term 'manifestly excessive' in respect of data subject requests (Art 12(4)) is poorly defined and will be open to wide ranging interpretation by different data controllers as well as national supervisory authorities. Therefore examples of what may be reasonably regarded as being a manifestly excessive request from a data subject would be helpful.

3. Notification requirements for data breach

The requirement in Art 31 to notify a supervisory authority within twenty four hours of 'becoming aware' of any data security breach is excessively burdensome - as is the extent of the information to be submitted as part of that notification process.

TfL would suggest that this creates a conflict for organisations attempting to formulate a response during the initial hours/days following a breach. Is the responsibility to notify the supervisory authority and keep them informed greater than the duty to investigate/contain the breach itself?

As a minimum, the period of time involved should be extended to forty eight hours and there should be some guidance or qualification of the obligation to notify linking it to the severity of the breach, or the harm caused (or likely to be caused).

4. Interaction between the DP Regulations and the Directive for processing personal information for prevention and detection of crime

Our organisation holds an individual's personal data for a number of different purposes. For some of TfL's activities, in some circumstances, (involving the processing of CCTV, payment card and passenger journey data), we would constitute a competent authority for the purposes of the prevention, investigation, detection or prosecution of a criminal offence or the execution of criminal penalties.

We are concerned that the personal data held on an individual could become subject to the obligations of both the Regulations and the Directive simultaneously, which would clearly be problematic from a compliance and data management perspective.

Appropriate guidance on how to manage personal information which for some reason becomes caught by both regulatory regimes would therefore be welcomed.