

**Consulted:** Richard Bevins

2.2 [REDACTED]

2.3



### 3 The GDPR

3.1 The GDPR will replace the Data Protection Act (DPA) 1998 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, and our understanding at present is that in the UK the nature of the obligations will not change after Brexit. While many of the main provisions and principles are consistent with the DPA, the GDPR also introduces several new concepts and, in general:

- strengthens the rights of individuals ('data subjects')
- increases obligations on organisations and their suppliers
- places more restrictions on organisations' use of personal data
- has a significantly enhanced enforcement regime, through a new power for the Information Commissioner to impose monetary penalties of up to 4 per cent of annual turnover for certain breaches of the Regulation

A summary of the GDPR is at Appendix I.

3.2 Despite the intention to provide a harmonised EU-wide basis for using personal data, the GDPR leaves many details to be decided by national parliaments or by regulators. No substantive progress has been made on this in the UK so the final nature of our obligations is not yet known. As the details to be decided include the age below which consent will be required from parents/guardians to process a child's personal data and the precise circumstances in which monetary penalties will be levied, this is a significant gap.

3.3 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 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. The latter aspect has implications for our use of the data collected from devices connecting to the Tube's wifi network and will require careful monitoring.

3.4 The GDPR's requirements will, amongst other things:



- 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 principle of 'accountability'. This involves ensuring that we know, and document in some detail, what personal data is being used, where and for what purpose. We must also identify and record the legal basis for processing such data (for example, the performance of a contract between TfL and the data subject)
- 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
- increase the amount of information we have to 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
- 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
- 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
- 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. Such incidents will have to be reported both to the Information Commissioner and, if they are exposed to significant risk as a result of the breach, to the affected individuals.

3.5 Complying with the GDPR poses significant challenges for any large customer-focussed, data-driven, organisation. Banks, financial services companies, retailers, utilities, tech companies and other transport operators (eg Eurostar, Network Rail, BA) are establishing dedicated GDPR compliance programmes. We have a good base to work from, having reached a relatively mature state of compliance with current legislation, and are building on this.

3.6 Within the TfL Group there are currently 16 legal entities acting as data controllers, all of which are now obliged to comply with the GDPR.



3.7 In the context of TfL's subsidiaries, given the level of potential fines and reputational harm associated with non-compliance with the GDPR, it's possible that a company director's failure to ensure protection of personal data would be considered a failure to properly exercise their statutory duties to promote the success of the company, and/or to exercise reasonable care, skill and diligence. This could potentially result in action for damages and/or termination or disqualification.

3.8 Preparatory work to date has included:

- a new project to identify contracts with current service providers which will need to be amended (up to 750 in total)
- changes to our procurement practices and standard contractual terms which ensure they are GDPR compliant
- the identification of 'privacy notices' and supplementary information provided to customers and employees which will need to be updated
- a standard DPIA template which is already being used by projects which may have a privacy impact
- a programme to refresh our existing Information Sharing Protocols and Procedures with police forces and other strategic partners
- 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.

3.9 But beyond this, we need to dedicate additional resource to programme management, further analysis of areas affected by the GDPR (to determine, for example, whether a particular business process involves profiling) and the production of the documentation that is required to track the use of personal data and demonstrate compliance. Some business areas are in the process of establishing projects (under a wider pan-TfL GDPR Compliance Programme) to undertake this and others should consider the need to do so too. Central co-ordination, common resources and specialist advice will be provided from the Privacy and Data Protection team, part of the Information Governance function in General Counsel.

The Assembly's Oversight Committee is carrying out an investigation into the use of personal data across the GLA Group and will be holding a hearing on this in September, with the Information Commissioner and representatives from TfL, the GLA and two privacy groups (Big Brother Watch and The Open Rights Group). Our preparations for GDPR implementation are likely to be scrutinised as part of the Committee's investigation.



4

[REDACTED]

4.1

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

- | [REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

4.2

[REDACTED]  
[REDACTED]  
[REDACTED]

5

[REDACTED]

5.1

[REDACTED] [REDACTED]  
[REDACTED]  
[REDACTED]



- 5.2 [REDACTED]
- 5.3 [REDACTED]
- 5.4 [REDACTED]

## 6 Next steps

### 6.1 We will:

- continue to develop and implement the GDPR Compliance Programme, working with projects established by business areas
- [REDACTED]
- [REDACTED]

## 7 Appendix

### Appendix I – GDPR Summary

[REDACTED]

## 8 Contact

Contact Officer: Howard Carter, General Counsel

Number: [REDACTED]

Email: [REDACTED]

