

**From:** Newman James (Privacy)  
**Cc:** [Meadows Lizzie](#); [Sloane Peter](#); [Nong Seeg](#); [McGirr Lee \(Privacy\)](#)  
**Bcc:** [Barrie Andy \(Prestige\)](#); [Barry John \(ST\)](#); [Blackwell Paul \(ST\)](#); [Boots Martin](#); [Bradley Peter \(ST\)](#); [Bradley Sarah \(TfL\)](#); [Brooker Robert](#); [Carlton Olivia](#); [Carman Tim](#); [Carter Charles](#); [Chapman Helen \(TPH\)](#); [Charlick Steve](#); [Clack Kevin](#); [Clarke Andrea \(Exc\)](#); [Conway John \(ST\)](#); [Cowperthwaite Paul](#); [Crowther Rebecca](#); [Daly Graham \(ST\)](#); [Davey Brian](#); [Diffenthal Jason \(LSTCC Manager\)](#); [Dixon Julie](#); [Everett Mike](#); [Fairhurst Malcolm](#); [Game Colin](#); [Geldard Mark \(ST\)](#); [Guernou Djamil](#); [Guild Simon](#); [Handley Tim \(Pensions\)](#); [Harper Caroline](#); [Hayward Siwan](#); [Johns Charlotte](#); [Kaye Mark IM](#); [Kenny Shamus](#); [King Andy \(Buses\)](#); [McCurry Pete](#); [McKenzie-Irvine Karen](#); [Mead James](#); [Sam Mullins \(LTM Director\)](#); [O'Neill Rory \(London Trams\)](#); [Osborn Richard](#); [Patel Nitesh IM](#); [Poulter Sarah](#); [Price Danny \(DLR\)](#); [Reston Kate](#); [Robinson Peter \(Reward & Pensions\)](#); [Sager Weinstein Lauren](#); [Sharples Esther](#); [Nielsen Simon](#); [St Martin Penny \(HR\)](#); [Stubbs Mike \(Overground\)](#); [Thompson Laila](#); [Thompson Andrew \(ST\)](#); [Thornhill Tamara](#); [Whitaker Mark](#); [Young Phil](#); [Behan Catherine](#)  
**Subject:** New EU data protection legislation - update for TfL Personal Information Custodians  
**Date:** 07 January 2016 13:11:00

---

Dear all,

Further to the email below, I thought it would be a good idea just to flag up a new piece of legislation – the “General Data Protection Regulation” – which is currently being finalised by the institutions of the European Union. The Regulation is intended to enable people to exercise greater control over their personal data and implement updated rules that will allow businesses to make the most of the opportunities of the “Digital Single Market”. Because it will effectively replace the UK Data Protection Act 1998 it will have a direct impact on TfL (both in terms of our operations and our relationships with various stakeholder groups). It is likely that this new law will be formally adopted in March/April of this year and from that point, a two year countdown to its full implementation will start to run, taking us to early 2018.

NB The pending referendum on the UK's continued membership of the EU does create a new element of uncertainty in relation to this new legislation; however, it makes sense for us to continue to plan for the eventuality that we will be impacted by the changes.

Based on the information currently available, it's now almost certain that the key provisions will include:

- Fines of up to 4% of annual global turnover for breaches of data protection rules (for TfL this would in theory mean a maximum penalty of £440 million, rather than the existing £500,000 limit);
- A more rigorous standard of consent for the processing of personal data will be one of “freely given, specific, informed and unambiguous” (ie a clear affirmative indication) and “explicit” consent for the use of sensitive personal data (ie special categories of personal data relating to ethnicity, health, alleged criminal offences, etc). There are some variations to this to avoid the process of obtaining consent online being “unnecessarily disruptive”;
- Personal data breaches will have to be notified to the relevant national privacy regulator “without undue delay” – and where feasible within 72 hours. Breaches unlikely to result in “a risk” to the rights and freedoms of data subjects will not need to be notified. The threshold for notifying the affected individuals would be breaches likely to pose “a high risk”;
- Easier access for individuals to their own data and greater transparency on how personal data is processed;
- An individual right to data portability (making it easier for consumers to transfer their personal data between service providers);
- A “right to be forgotten” when an individual no longer wants their data to be processed (it will have to be deleted unless there are legitimate grounds for retaining it);
- Tougher restrictions on the use of profiling and the collection and use of personal data relating to individuals under the age of 16 (which will require the consent of a parent/guardian and reasonable efforts to verify that third party consent), but with flexibility for Member States to lower the threshold to 13 years of age;
- Joint and several liability for service providers (data processors) processing personal information on behalf of a data controller. This may have an impact on large-scale procurement and outsourcing activities where liability currently remains exclusively with the data controller (although this is already mitigated by TfL and other data controllers through the use of appropriate contractual indemnities);

- Greater emphasis on the requirement for organisations to adopt the concepts and practices of “privacy by design” (ie using Privacy Impact assessments which help to ensure that data protection safeguards are built into products and services from the early stages of development) and “privacy by default” (eg the use of techniques such as pseudonomysation to support big data innovation while protecting privacy);
- The removal of the current requirement for data controllers (including TfL and most of its operating subsidiaries) to register with the relevant national privacy regulator. Instead they will be required to document evidence of their compliance with the new legal framework and make that evidence available for the regulator to inspect (on request);
- Promotion of a risk-based approach to compliance (to avoid a one-size-fits-all set of obligations).

To date, in anticipation of the GDPR, we've already made good progress in terms of preparing TfL for a number of these changes. This has involved updates to standard privacy and data protection ITT questions and contract clauses used to procure services from new TfL suppliers; the development of a Privacy Impact Assessment checklist which is being integrated into the Pathway project management tool; expanded content within the TfL website and intranet privacy pages; the creation of additional information sharing protocols and procedures with partner organisations engaged in law enforcement activities; the adoption of a framework agreement with Experian covering the provision of ID theft protection services in the event of a breach; updates to TfL's privacy and data protection eLearning; a series of planned changes to the TfL Data Protection Policy; site visits to service providers and suppliers processing personal data; and a shift towards the use of an opt-in (rather than opt-out) approach to obtaining consent to the processing of personal data.

Once the full text of GDPR is available we will be able to identify any further measures TfL needs to adopt; and begin to provide detailed advice/guidance to individual business areas. As mentioned above, TfL and other data controllers have just over two years to prepare for the various changes to the way in which they collect and use personal information.

Please let me know if you have any questions or comments re: any aspect of the above.

Best wishes,

James

**James Newman CIPM CIPP/E | Privacy and Data Protection Manager**

Transport for London | Windsor House, 42-50 Victoria Street, London SW1H 0TL

*Personal information plays a critical role in keeping London moving. Take a look at the [Privacy & Cookies](#) section of the TfL website to find out more. If you work for TfL or one of its subsidiaries visit [Managing personal information](#) to view a summary of your privacy and data protection responsibilities.*

---

**From:** Newman James (Privacy)

**Sent:** 04 November 2015 11:58

**Cc:** Meadows Lizzie; Sloane Peter; Nong Seeq; McGirr Lee (Privacy)

**Subject:** TfL Personal Information Custodians

**Importance:** High

Dear colleague,

Following a recent internal audit focussed on privacy and data protection compliance, my team was tasked with the following management action:

***“In the absence of an Information Asset Register as originally envisaged, the Privacy and Data Protection Team will compile a comprehensive list of all the business areas where personal data is processed, identifying a responsible senior manager for each area.”***

Consequently, you have been identified as one of these 58 individuals, ie a 'Personal Information Custodian'. This is because you have day to day responsibility for decisions about the way in which personal information is collected, stored, analysed or otherwise 'processed' by TfL systems and/or business processes (including those used by outsourced service providers).

Please note, that at this point we are not asking you to do anything or to take on any new responsibilities..! In most cases, you will already be someone we work with on a regular basis regarding privacy and data protection compliance issues (eg privacy notices, data processor contract terms and conditions, data sharing agreements, data breaches, subject access/third party data requests, etc). However, if you aren't already familiar with them, you may find it useful to take a look at the following online information resources:

- TfL website: [www.tfl.gov.uk/privacy](http://www.tfl.gov.uk/privacy)
- TfL Management System: [Managing personal information](#)

Going forward, we intend to use this group of key contacts to communicate any significant changes to either TfL policy or the law, which may impact upon how your business area processes personal information. If you have any questions about the above, or do not believe you are the right person from within your business area to be included as a Personal Information Custodian, please let me know.

Requests for advice and guidance on privacy and data protection matters should continue to be directed to the following individuals:

- [Lizzie Meadows](#) and [Lee McGirr](#): (personal information relating to customers, taxi/private hire licensees and members of the public)
- [Peter Sloane](#) and [Seeq Nong](#) (personal information relating to our workforce, job applicants and pension scheme members/beneficiaries)

Best wishes,

James

**James Newman | Privacy and Data Protection Manager**

Transport for London | Windsor House, 42-50 Victoria Street, London SW1H 0TL

*Personal information plays a critical role in keeping London moving. Take a look at the [Privacy & Cookies](#) section of the TfL website to find out more. If you work for TfL or one of its subsidiaries visit [Managing personal information](#) to view a summary of your privacy and data protection responsibilities.*