

From: [Newman James \(Privacy\)](#)
To: [Carter Howard](#); [Bevins Richard](#); [Clarke Andrea \(Exc\)](#); [Curry Justine](#); [Everitt Vernon](#); [Delgadillo Francisca](#); [Townsend Steve IM](#); [Verma Shashi](#); [Hanson Michele IM](#); [Young Phil](#); [Emmerson Garrett](#); [Burton Steve \(ST\)](#); [Blake Peter](#); [Quincey Andrew \(Director, Commercial\)](#)
Cc: [Adcock Emma](#); [Shrestha Rumi](#); [Lee Stuart](#); [Harrison-Cook Victoria](#); [Walker Clive \(Internal Audit\)](#); [Origbo Diji](#)
Subject: New EU data privacy and security legislation
Date: 17 December 2015 14:25:48

Dear all,

Included below are some key points relating to three new pieces of legislation currently being finalised by the institutions of the European Union. All three are expected to be approved by the European Parliament in separate votes early next year (at which point the full texts will be made available). All three will have a direct impact on TfL (both in terms of our operations and our relationships with various stakeholder groups). One of the pieces of legislation is a Regulation and will therefore have 'direct effect' on the UK (ie no domestic law needs to be passed), the other two are Directives and therefore the UK government will be required to bring forward domestic legislation to implement their provisions.

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.

THE GENERAL DATA PROTECTION REGULATION (GDPR)

On 15 December (after nearly four years of negotiation) the EU institutions (the Commission, Council and Parliament) reached agreement on the new General Data Protection Regulation (which will replace the current EU Data Protection Directive and UK Data Protection Act). 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" as a result of harmonisation and improved levels of consumer confidence.

The compromise text has now been passed to the Council (made up of ministers and officials representing each of the Member States) and the European Parliament for ratification. The Parliament's Civil Liberties, Justice and Home Affairs Committee, the lead committee for the proposals voted to approve them (by 48 votes to 4, with 4 abstentions) this morning (17 December) and the European Parliament will vote in plenary session during March/April 2016.

Once the final text has been approved and translated into all of the EU languages, it will be formally signed by the Presidents of the Parliament and the Council, then published in the Official Journal. From that point, a two year lead in time will start to run, taking us to early 2018. The Regulation will have direct effect in Member States (the aim of the reform being a harmonised EU regime) although there are some areas where individual Member States will have a discretion to impose stronger or weaker rules.

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 the 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 pseudonymisation 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).

There will be additional associated with the GDPR (which runs to 200 pages), so further information will be provided once we've had an opportunity to review the full text. 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.

THE POLICE AND CRIMINAL JUSTICE DATA PROTECTION DIRECTIVE

This Directive forms part of a legislative package alongside the GDPR and covers data protection standards for the processing of personal information in the context of law enforcement and prosecutions (including the prevention and detection/investigation of crime; and cross-border co-operation between EU member states intended to combat crime and terrorism). The fact that this is a Directive means that member states have a greater degree of flexibility in terms of taking into account their specific law enforcement needs and the different legal structures/traditions in place across the EU.

The impact of this Directive on TfL isn't yet clear, however our powers of prosecution for fare evasion and our extensive personal data (and intelligence) sharing activities with law enforcement agencies may bring us directly within the scope of the legislation. It is intended to regulate the processing of all personal data associated with policing or criminal justice purposes, regardless of whether they are a victim, witness, suspect or convicted criminal. All law enforcement processing in the EU will have to comply with the principles of necessity and proportionality, with appropriate safeguards being implemented for affected individuals.

The process through which the draft Directive will be approved is the same as that which applies to the GDPR (it was also approved by Parliament's Civil Liberties, Justice and Home Affairs Committee this morning; by 53 votes to 2, with 1 abstention), however individual EU member states will then have to draft and pass domestic legislation which implements the provisions of the Directive (and this will have to be done by a specified date).

THE NETWORK AND INFORMATION SECURITY DIRECTIVE (NISD)

On 7 December 2015, the EU institutions also reached an agreement on the text of the NISD which is intended to establish common rules to strengthen cybersecurity across the EU. The Directive, originally proposed in 2013 as part of the EU Cybersecurity Strategy, is focussed on protecting the technological infrastructure that underpins critical national infrastructure, and achieving a minimum security standard across all EU countries. It sets out a common baseline level of mandatory cybersecurity measures for operators of essential services and key infrastructure and obliges them to report details of serious cyber-attacks and data breaches to a specified national authority/regulator (it is unclear at this stage whether this will be an entirely new regulator in the UK, or whether the role will be allocated to/split between, existing regulators depending on the sector concerned, eg the ICO, Ofcom, FCA, etc).

The NISD lists a number of critical sectors in which operators of essential services are active, such as energy, transport (including rail, water, road and air), finance, water supplies and healthcare. Within these sectors, individual EU member states will identify those operators providing essential services, based on a set of criteria laid down in the Directive (we can safely assume that TfL will be included in that list). This reflects the degree of risk that any disruption to their services may pose to "critical societal or economic activities".

EU member states will be required to provide for sanctions for failure to comply with the NISD. Such sanctions will have to be effective, proportionate and "dissuasive". These are likely to include significant fines (this is a completely separate fines regime from the one created by the GDPR specifically in relation to personal information). It may also be worth adding that there is an assumption among the EU institutions and member state governments that operators of essential services covered by the Directive are already taking cybersecurity very seriously and that the Directive shouldn't involve any significant burden/upheaval for them.

Each EU country will also be required to set out a cybersecurity strategy (the UK has already done a considerable amount of work on such a strategy). EU member states will also step up their co-operation on cybersecurity, supported by a pan-EU group which will support strategic cooperation and exchange of best practice among member states (ENISA, the EU's agency for Network and Information Security, will also play a key role in supporting this new approach). A network of national computer security incident response teams (CSIRTs) will be set up to promote co-operation and the sharing of information and intelligence on cyber threats/risks.

The process through which the draft Directive will be approved is similar to that which applies to the other two pieces of legislation mentioned above (although the Parliament's Internal Market Committee is the lead committee for this particular Directive), individual EU member states will then have to draft and pass domestic legislation which implements the provisions of the Directive within 21 months. After this, they will have a further six months to identify their operators of essential services.

WORK IN PROGRESS AND NEXT STEPS

To date, in anticipation of the GDPR work has been carried out to create an enhanced Privacy and Data Protection Compliance Programme. This has involved updates to standard privacy and data protection ITT questions and contract clauses; 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 identify any further measures required.

With regards to preparing for the potential impact of the NISD, much of the work IM's Cyber Security and Incident Response Team have initiated will be of direct benefit (including their work on an incident response plan which will also support compliance with the GDPR). It could be helpful to refer

to these anticipated legal obligations as an additional driver for the actions arising from the cybersecurity Data Summits (the first of which took place on 13 November and the second of which is scheduled to take place tomorrow, 17 December).

It may also now be appropriate to start thinking about the most appropriate way to brief the Leadership Team; Audit & Assurance Committee; Customer Pillar Group; Value Pillar Group; and Technology and Data Pillar Group on these anticipated changes, later in the new year.

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.