15 SEPTEMBER 2016

Data Protection Update - GDPR

Seeq Nong, Privacy Adviser, Privacy and Data Protection Team

EU General Data Protection Regulation

- New law, approved in April 2016 by the European Parliament
- Comes into force on 25 May 2018
- Replaces the current Data Protection Act 1998
- Introduces tougher, stringent obligations on organisations, more protection for individuals
- Brexit implications: Keep calm and carry on

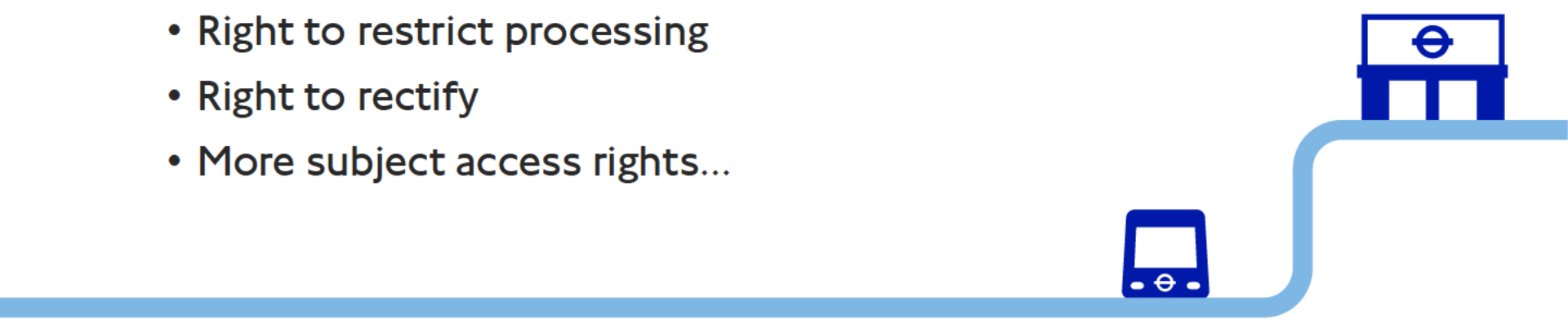
What are the key changes

- Fines of up to 4% of annual turnover (or €20,000,000) for serious breaches of the GDPR.
- Personal data breach notification - Data controllers must notify the supervisory authority (Information Commissioners Office) 'without undue delay' or within 72 hours of being made aware that personal data has been lost; if there is a high risk to individuals then they must be informed
- Expanded scope - applies to all data controllers and processors (service providers) established in the EU and organisations that target EU citizens;
- New obligations on data processors - they become an officially regulated entity;
- Consent - must be 'freely given, specific, informed and unambiguous; explicit consent for processing sensitive personal data;
- Accountability - obligations include: documenting data processing activities, policies; building in data protection safeguards in new systems or processes, including privacy friendly default settings (set at highest level) on for example, social networks and apps;
- Privacy Impact Assessments

New rights to data subjects

These rights are substantial.....

- Right to be forgotten or Right to erasure
- Right to data portability (receive back their personal information in a structured and commonly used format so that it can be transferred to another data controller)
- Right to object to profiling – right not to be subject to decisions solely on automated processing
- Right to restrict processing
- Right to rectify
- More subject access rights...



Changes to Subject Access Requests (SARs)

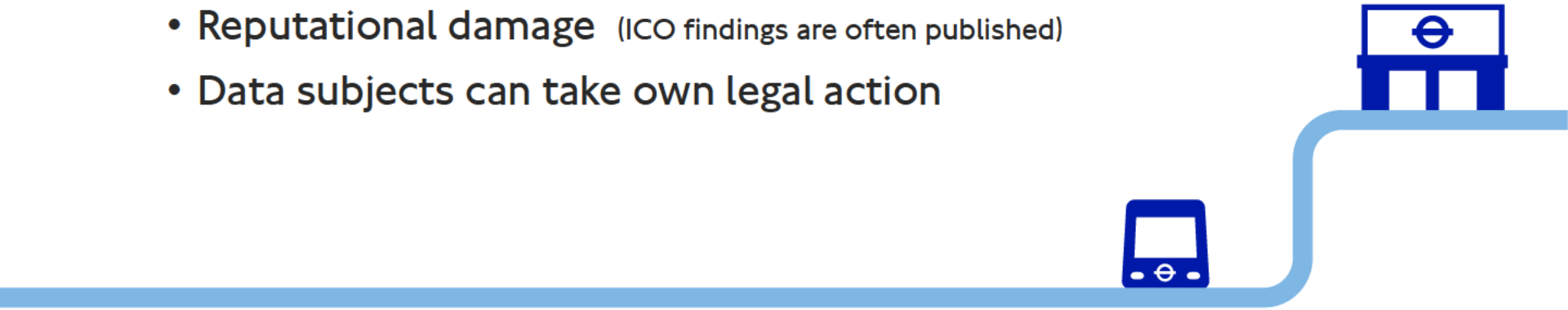
- Will have just one month to process (instead of 40 days!)
- FREE – can no longer charge £10
- Exemptions not to comply – manifestly unreasonable or excessive requests can be charged or refused
- When supplying the information, must provide all of the following (text in red is new requirement under the GDPR:-

✓ Purpose of processing (e.g staff administration)
✓ Categories of data processed
✓ Exemptions (if withholding or redacting information)
✓ Description of the source of the information (e.g individuals data subjects have named on their request and DA)
✓ Any regulated automated decision making
✓ Right to lodge complaint to the ICO
✓ Data retention period
✓ Right to have inaccurate data corrected
✓ Right to object to processing
✓ Who the information is shared with (eg international organisations or countries outside the EU)

Consequences of not complying

ICO investigation can lead to:-

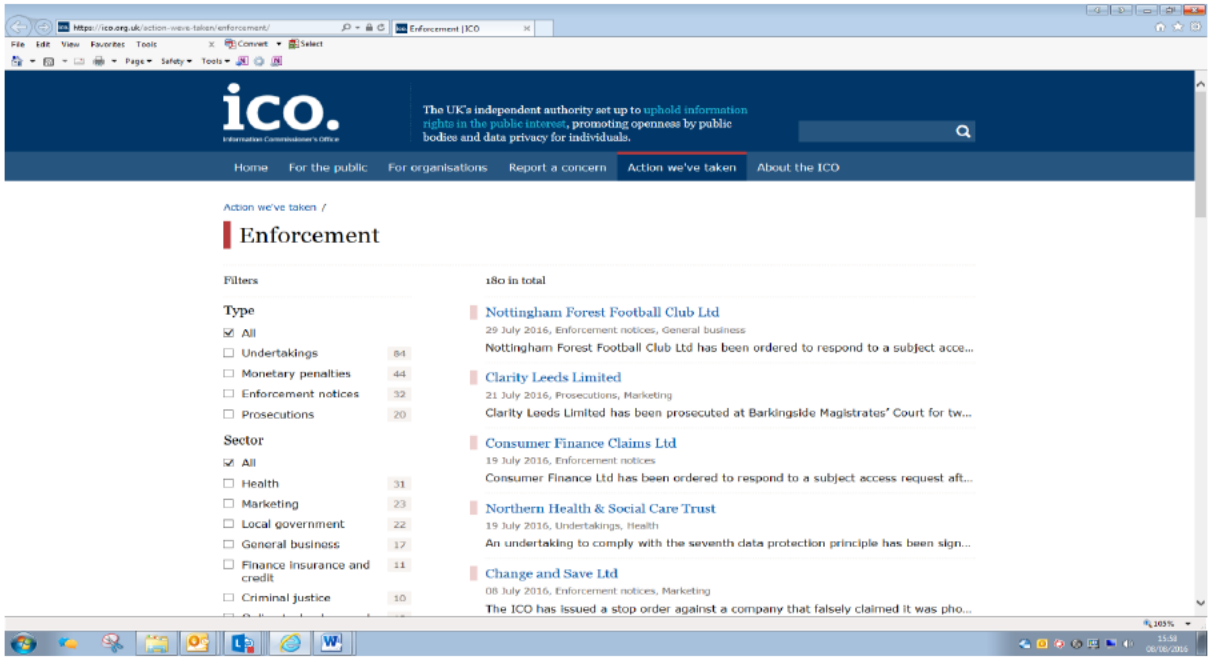
- Fines (current max £500k under DPA, 4% turnover under GDPR)
- Enforcement notice (is a criminal offence to ignore these)
- Undertaking
- Inspection and audits
- Prosecution – corporate or individual
- Reputational damage (ICO findings are often published)
- Data subjects can take own legal action



When things go wrong

- 2015 – TfL employee prosecuted by the ICO for unlawfully accessing Oyster card records of family members. Convicted and fined £1000 plus costs.
- 2015 – TalkTalk cyber attack, 157,000 customer personal details compromised. ICO currently investigating.

www.ico.org.uk

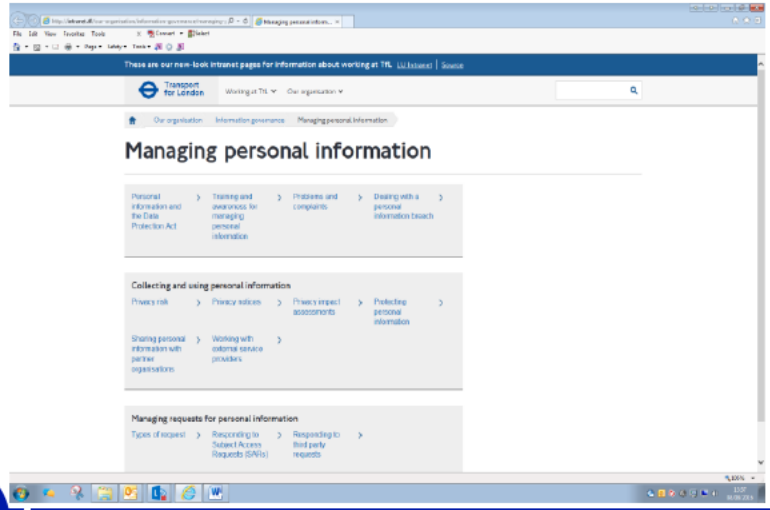


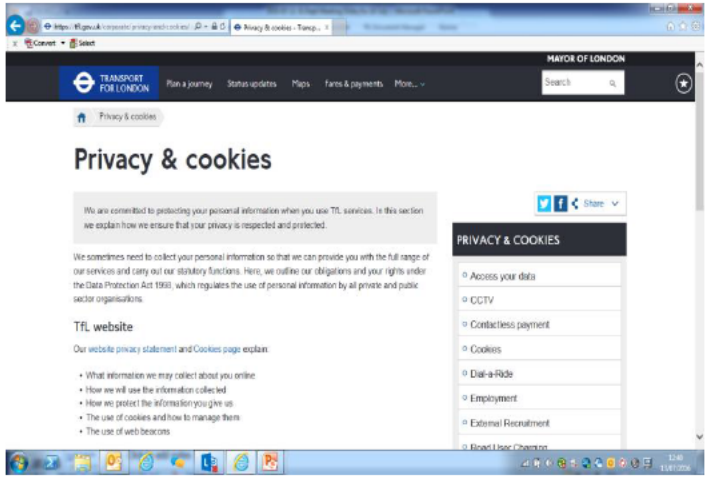
TfL Privacy and Data Protection Policy (Updated March 2016)

Main changes are:-

- PIA's to be carried out as part of the development of new business or IT systems where personal information will be processed
- Mandatory privacy awareness training every year
- Serious or repeated breaches of the policy may be treated as misconduct
- TfL will be open and transparent about how personal information is used
- Data breaches should be reported to the Cyber Security and Incident Response Team

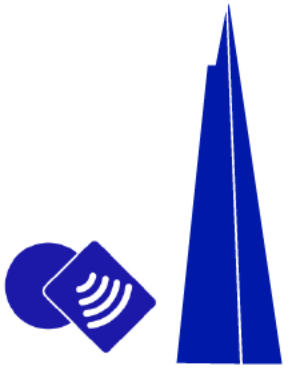
If you're involved in processing personal information, whether it's our customers, other members of the public, or colleagues, take a look at the policy and supporting information on the Managing personal information section of the TfL Management System and the Privacy & Cookies section of the TfL website.





Personal data volumes at TfL (as of Nov 2015)

- **26 million** retail Oyster cards used in 2015 (includes **4.1 million** 'registered' cards)
- **8 million** contacts in our customer database (includes **4.5 million** email addresses - **309 million** service info emails sent in 2015)
- **7 million** contactless payment cards used in 2015
- **1.7 million** active Congestion Charge/Low Emission Zone customer records (includes **455,000** discount/auto-pay accounts)
- **1.6 million** Oyster concessionary photo cards used in 2015
- **200,000** registered Santander Cycles users
- **100,000** licensed taxi/private hire drivers
- **84,000** TfL pension scheme members
- 47,000 registered Dial-a-Ride users
- 27,000 members of staff
- 21,000 CCTV cameras
- 1,400 Automatic Number Plate Recognition cameras



Contact

Privacy and Data Protection Team, Information Governance, General Counsel

privacy@tfl.gov.uk