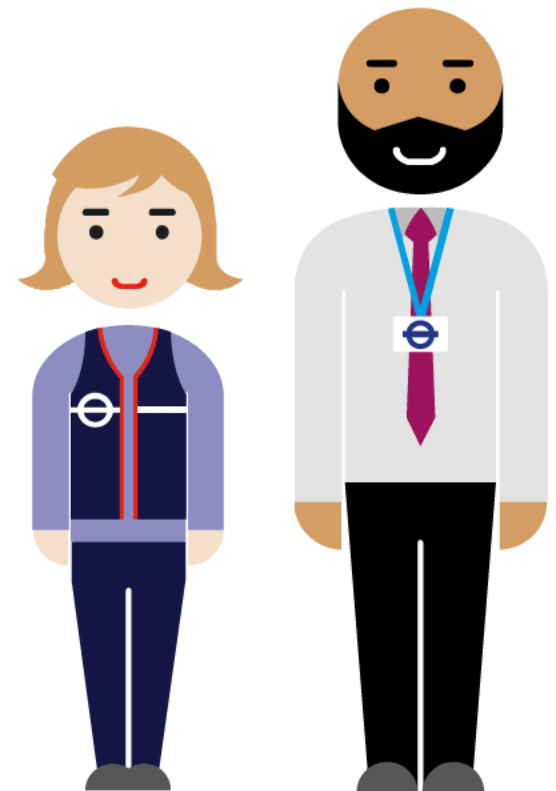


TUESDAY 14 MARCH 2017

# The new General Data Protection Regulation

A briefing for the TfL People Policy Review Group

James Alexander  
Head of Privacy and Data Protection



EVERY JOURNEY MATTERS

# What is the new EU General Data Protection Regulation (“GDPR”)..?



# The General Data Protection Regulation

- Replaces the EU Data Protection Directive 1995 and the UK Data Protection Act 1998
- Harmonised legal framework to support a modern digital economy
- Comes fully into effect on 25 May 2018
- UK has confirmed it will implement GDPR
- Many concepts stay the same (personal data, data processing, data controller/processor, etc)



## Key changes in the law

- Significantly increased fines; two tiers with a maximum of either:
  - **2%** of annual turnover (internal record keeping; processor agreements; security; breach notification; DP by design/default)
  - **4%** of annual turnover (data protection principles/consent/data subject rights/international data transfers)
- TfL's annual turnover is around £10billion



## Key changes in the law (continued)

- Consent – clear affirmative action and must be freely given, specific, informed and unambiguous (though consent is not the only basis for processing personal data...)
- Accountability/record keeping – detailed documentation recording processing
- Data breach notification – serious breaches must be reported to ICO within 72 hours



## Key changes in the law (continued)

- Right to erasure – in certain circumstances
- Right to object to processing/profiling – in certain circumstances
- Subject Access – no fee (currently £10); data controllers must respond within one calendar month (currently 40 calendar days)
- “Privacy by design” – eg Data Protection Impact Assessments for new projects
- Stronger data processor agreements



**Why does the new law matter to TfL in the context of job applicant and employee data..?**



## We have lots of personal data about...

- Current/former employees (including, equality data, health related information, drug and alcohol test results, etc)
- Holders of staff nominee travel passes
- Unsuccessful job applicants/candidates
- TfL pensions scheme members
  - active members
  - deferred members
  - Pensioners/beneficiaries



## What could happen if we don't comply?

- Monetary penalties or other regulatory enforcement action taken by the ICO
- Civil litigation (including class actions)
- Adverse media coverage
- Reputational damage
- Loss of trust and confidence amongst our people and/or customers
- Political consequences (the Mayor, Assembly Members, MPs, councillors)



**What are we doing to prepare for the new law..?**



## We started preparing early...

- New GDPR commercial contract clauses
- TRUSTe Data Protection Impact Assessment tool procured and deployed
- Breach services framework with Experian
- Updated Information Sharing Protocol and Procedure templates
- Colleagues being briefed on the GDPR
- Being more open and transparent about how we use personal data – for example...



# Transparency – how we use employee data

**TRANSPORT FOR LONDON** Plan a Journey Status updates Maps Fares & payments More... Search

Privacy & cookies Employment

## Employment

The information on this page explains how Transport for London and its subsidiaries including London Underground Limited (TfL), use your personal information when you become an employee. It also describes how long that information is kept and the circumstances in which we might disclose it to a third party.

▼ Personal information we hold      ▼ Sharing personal information  
 ▼ How we use personal information      ▼ Overseas processing  
 ▼ Length of time we keep information      ▼ How to access personal information  
 ▼ Keeping personal information secure

### Personal information we hold

The personal information we hold includes:

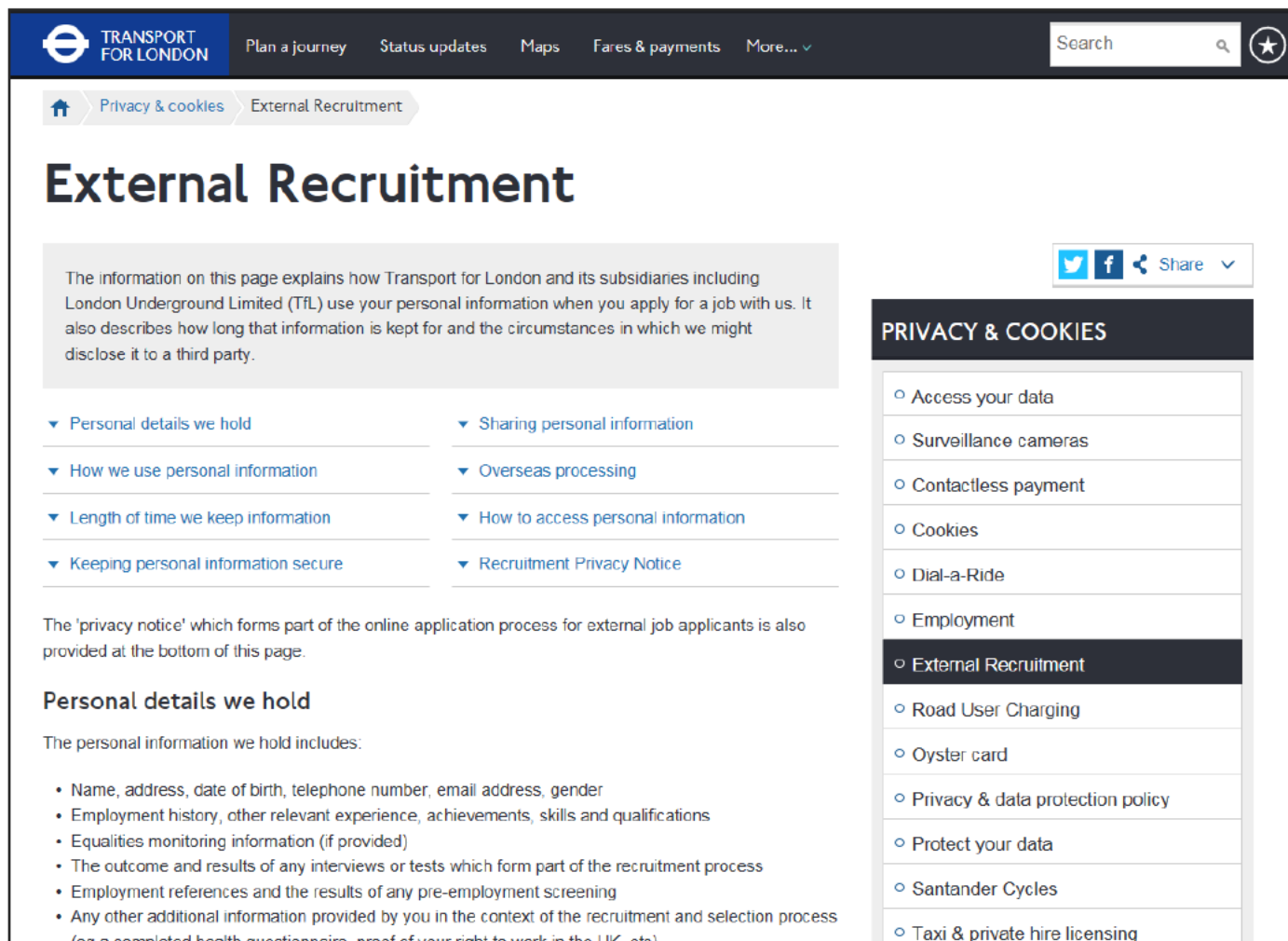
- Name, address, date of birth, telephone number, email address, gender, proof of your right to work in the UK
- Employment history, other relevant experience, achievements, skills and qualifications
- Employment references and the results of any pre-employment screening
- The outcome and results of any interviews or tests which formed part of the recruitment process
- Terms and conditions of employment, contract variations, current employment history
- Information about your conduct, performance, training and development
- Pay and pension details, national insurance number, tax coding and details of the bank or building society account into which your salary is paid
- Details of your employee benefits (eg membership of private medical insurance or childcare voucher)

### PRIVACY & COOKIES

- Access your data
- Surveillance cameras
- Contactless payment
- Cookies
- Dial-a-Ride
- **Employment**
- External Recruitment
- Road User Charging
- Oyster card
- Privacy & data protection policy
- Protect your data
- Santander Cycles
- Taxi & private hire licensing



# Transparency – how we use applicant data



The screenshot shows the Transport for London website's 'External Recruitment' page. The header includes the TfL logo and navigation links: 'Plan a journey', 'Status updates', 'Maps', 'Fares & payments', and 'More...'. A search bar and a star icon are on the right. Below the header, a breadcrumb trail shows 'Home' > 'Privacy & cookies' > 'External Recruitment'. The main heading is 'External Recruitment'. A text box explains that the page details how TfL and its subsidiaries use personal information for job applications. Below this, two columns of links are provided: 'Personal details we hold', 'How we use personal information', 'Length of time we keep information', 'Keeping personal information secure', 'Sharing personal information', 'Overseas processing', 'How to access personal information', and 'Recruitment Privacy Notice'. A paragraph states that the 'privacy notice' is part of the online application process. The 'Personal details we hold' section lists the types of information held, including name, address, date of birth, telephone number, email address, gender, employment history, achievements, skills, qualifications, equalities monitoring information, interview results, employment references, and any other additional information provided. On the right, a 'PRIVACY & COOKIES' sidebar lists various topics: 'Access your data', 'Surveillance cameras', 'Contactless payment', 'Cookies', 'Dial-a-Ride', 'Employment', 'External Recruitment' (highlighted), 'Road User Charging', 'Oyster card', 'Privacy & data protection policy', 'Protect your data', 'Santander Cycles', and 'Taxi & private hire licensing'. Social media sharing icons for Twitter, Facebook, and a general 'Share' button are also present.





## GDPR awareness briefings for HR

- HRS Senior Adviser Team
- HR Strategic Planning and Governance
- Recruitment
- ERP Design Authority
- Individual PMAs
- PMA team briefings planned



**...we have lots more to do by 25 May 2018!**

HR specific tasks:

- Review of HR policies to identify any potential GDPR issues
- Review of current terms and conditions of employment to ensure these cover personal data processing activities

Wider tasks:

- Pan-TfL personal data mapping exercise



## ...there is still lots more to do! (continued)

- Over 30 privacy notices to be updated
- 28 information sharing agreements to be reviewed and updated
- Relevant website and Intranet content to be reviewed and updated
- “My role in privacy and data protection” eLearning to be reviewed and updated
- Privacy and Data Protection Policy to be reviewed and updated



## Contact

Privacy and Data Protection Team  
Windsor House  
42-50 Victoria Street  
London SW1H 0TL

[privacy@tfl.gov.uk](mailto:privacy@tfl.gov.uk)

