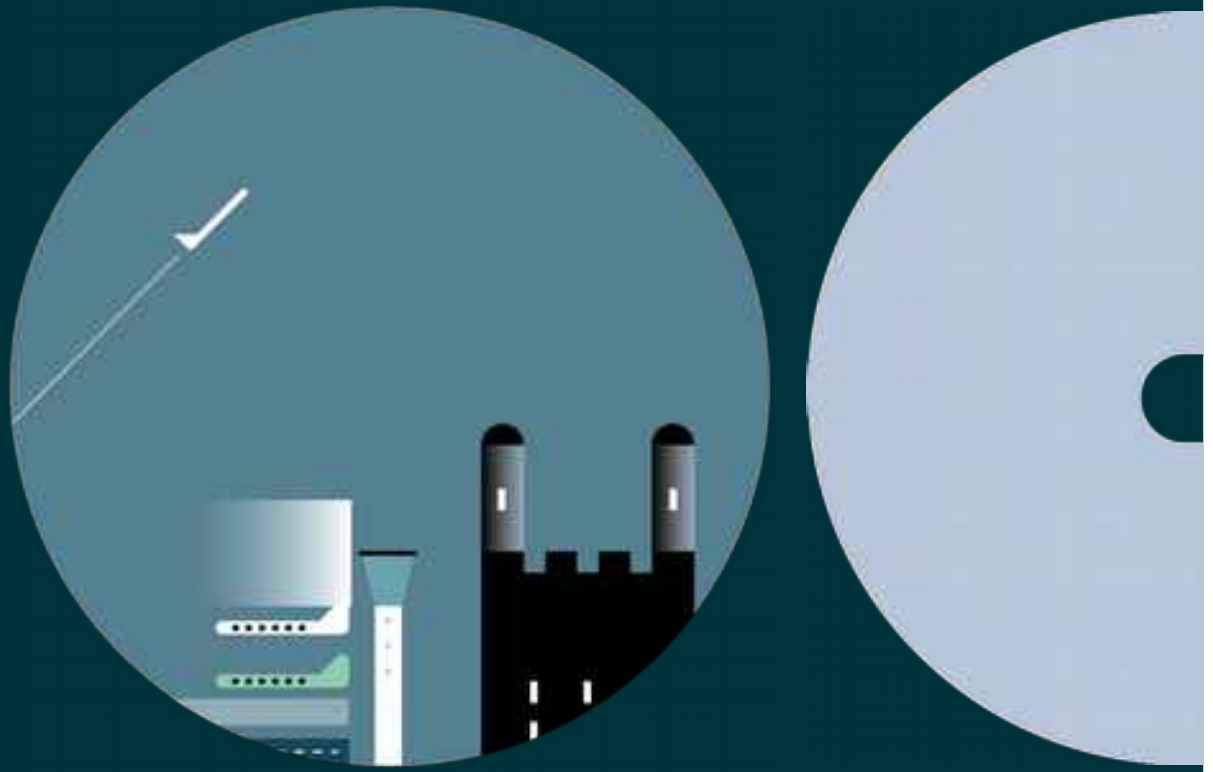
Data privacy and IoT

Georgina Graham

21 July 2017



What we're going to cover

- What are the relevant laws?
- Key concepts / principles
- Key privacy challenges in IoT
- Practical next steps and reasons to comply

What are the relevant laws?

Main EU law that currently regulates personal data:

- EU Data Protection Directive (implemented in the UK by Data Protection Act 1998)
- General Data Protection Regulation (GDPR)

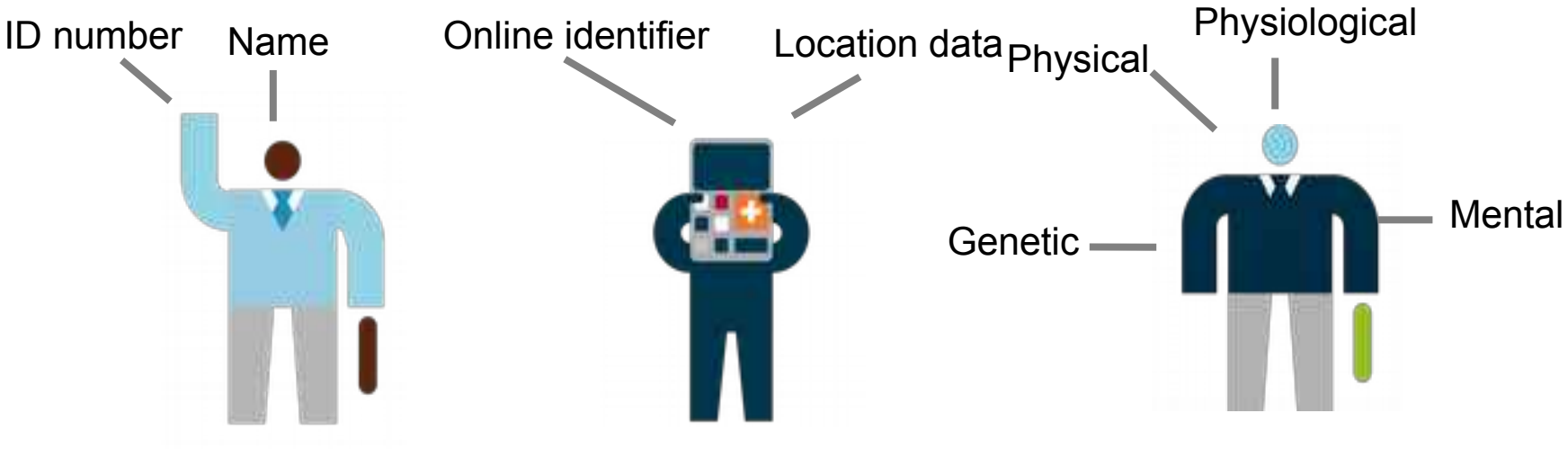
Other laws that don't just regulate 'personal data':

- EU e-Privacy Directive (implemented in the UK by the Privacy and Electronic Communications Regulations 2003)
- EU Network and Information Security Directive – coming soon

Key concepts / principles

Is "personal data" being "processed"?

Information relating to a living individual directly or indirectly **identifiable** from that information



- **Sensitive Personal Data** – Religion, health, sex life, trade union membership, political beliefs, criminal conviction/proceedings
- **Biometric data**, e.g. data collected using facial recognition or voice recognition technology, fingerprints, video surveillance – this category of data is certainly personal data and may also be sensitive personal data. Regulators have stressed the importance of proportionality and security when collecting biometric data.
- **Processing** – Any handling of personal data

Key concepts / principles

Who's who?

Data controller

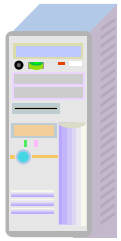
Decides alone, jointly or in common with another how and why data processed

Outsource processing

Data collection

Data processor

Processes data under data controller's instruction



Data subjects

Data protection principles under the GDPR

Key data privacy challenges in smart buildings (1)

- **Transparency**
  - Complex and unknown uses and sharing of data, future changes, secondary uses of data, more detailed and potentially intrusive profile creation, risk of re-identification, automatic collection of data
  - Constraints of technology, no screen/space and timing restrict delivery of adequate privacy notices and policies
- **Consent**
  - Is consent required? If so, how will fully informed, freely given and specific consent be given?
- **Conditions for processing non-sensitive personal data**
  - When is processing necessary for a contract? Can legitimate interests of controller outweigh risks to individual privacy rights?

Key data privacy challenges in smart buildings (2)

- **Sensitive data**
  - "Sensitive" according to GDPR and individual perception
  - Requiring greater care in handling and explicit consent
- **Data quality and retention**
- **Data minimisation**
- **Collecting only what is needed, not potentially useful/interesting data**
- **Multiple data controllers and data processors**
  - Identifying all stakeholders, their roles and interfaces, uses of data and any third party monitoring, entering into contracts
- **Data subject rights and access**
- **Security risks and vulnerabilities**

Practically, what does all this mean?

What, why, who, where and for how long?

Map potential data flows

Adopt Privacy by Design principles

Governance

Clear lines of responsibility and accountability

Know and control your supply chain

Why comply?
The good, the bad and the ugly…

- The good:
  - There are **positive** and **practical commercial benefits** of complying with data privacy laws.
  - In particular, it allows you to create **value** from data by maximising revenue generation opportunities, driving efficiency savings and so on.
- The bad:
  - Regulators have a range of investigative, corrective, authorisation and advisory **powers** (as well as the power to issue fines)
  - Right to claim **compensation** from the controller or processor
  - Potential **reputational damage**
- The ugly:
  - **Fines** applicable by regulators (significantly increased under the GDPR):
    - higher threshold = up to higher of €20m or 4% of worldwide turnover
    - lower threshold = up to higher of €10m or 2% of worldwide turnover

Contacts

Georgina Graham
Senior Associate
Data Protection

T +44 117 917 3556
georgina.graham@osborneclarke.com