

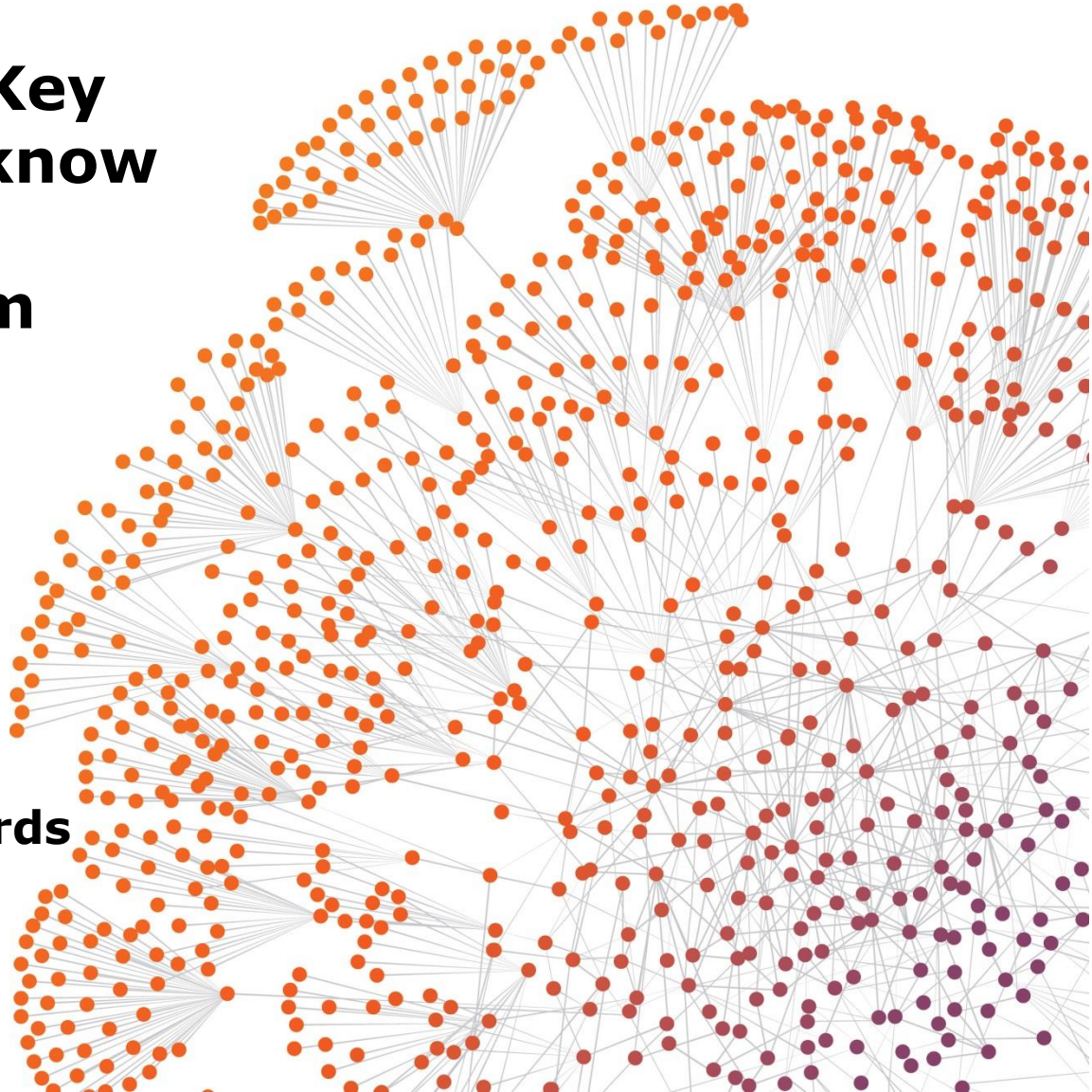


# **GDPR Countdown– Key things you need to know**

**IQCS Working Forum**

**25<sup>th</sup> May 2017**

**Dr Michelle Goddard**  
**Director of Policy & Standards**

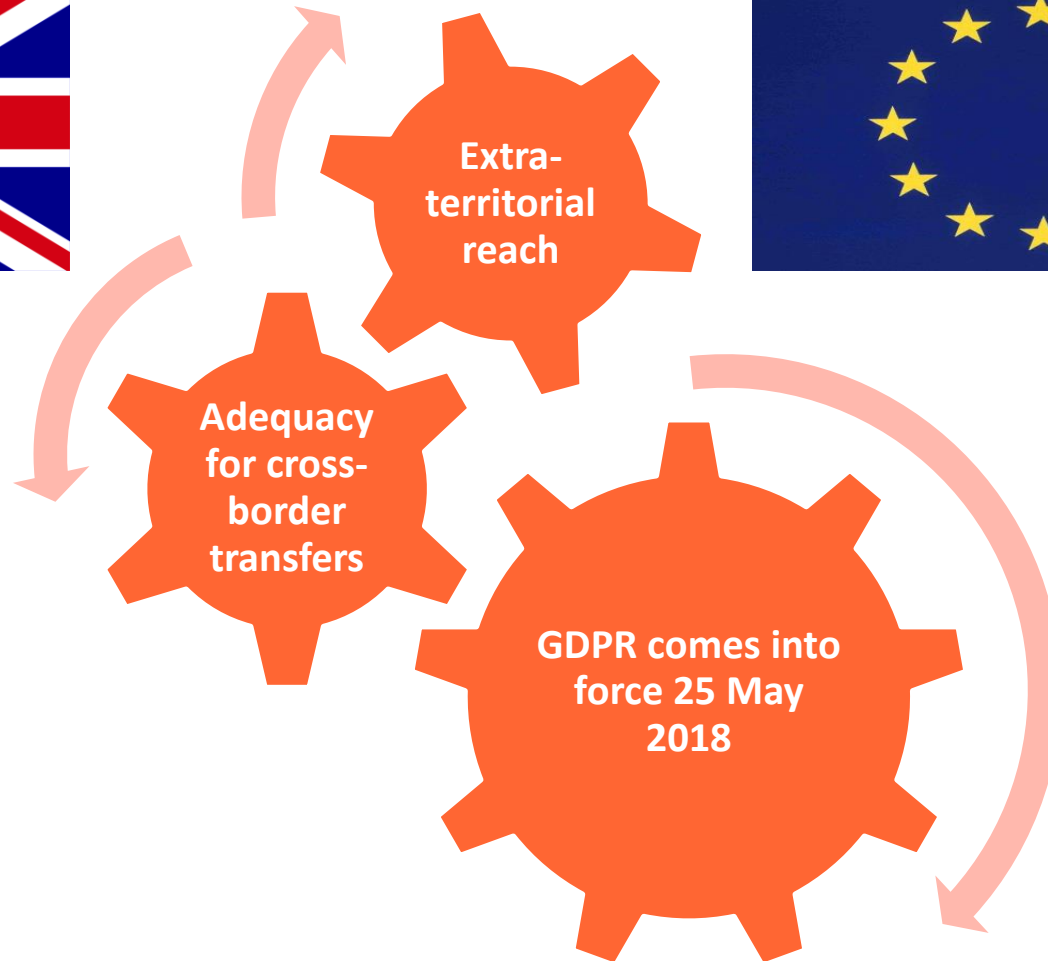
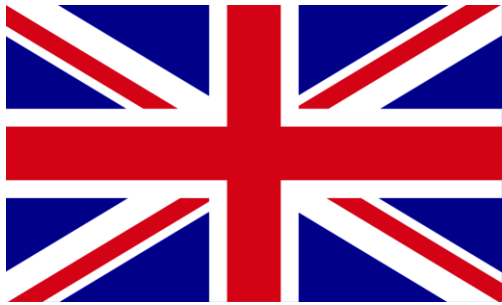


# GDPR: New harmonised framework across EU



From  
Directive to  
Regulation

# .... but what about Brexit?



# GDPR: Wider scope of data categories



## Personal Data

Any information relating to identified or identifiable natural person

Expanded to include online identifiers

Can use standard processing grounds

## Sensitive Personal Data

Special categories of data including health data, political opinions

Expanded to include biometric and genetic data

Requires explicit consent unless falls within limited exemptions

# GDPR: Greater business accountability even for small businesses

---



## Increased obligations

- Demonstrate compliance
- Embed privacy by design and default
- Detailed written internal records
- Privacy Impact Assessments
- Data Protection Officers

## Reduced burden

- No notifications to ICO



# GDPR: Direct obligations on data processors



## Data Controller (DC)

- **New mandatory contract terms** (include security measures, right of audit of DP, sub-processor approvals)
- **Full statutory liability** and shared liability

## Joint Data Controller

- **Explicit recognition of joint DC**
- **New mandatory contract terms** (include security of measures, right of audit of DP etc and how data subjects can exercise rights and who provides information)
- **Full statutory liability** but shared liability

## Data Processor (DP)

- **New mandatory contract terms** (include seek approval of DC for appointment of sub-processor and data transfers out of EEA)
- **Direct liability** now includes full range of enforcement action in addition to liability for breach of contract

# GDPR: Strengthened individual rights



## New

- Right to data portability
- Right to erasure/"be forgotten"
- Right to restrict processing

## Strengthened

- Right to access data
- Right to information in notices
- Right to withdraw consent
- Right to object to processing
- Right not to be evaluated by automated processing
- Right to rectification (of inaccurate data)

***Need to promote all these rights to individuals***

# GDPR: Mandatory breach notification



## ➤ **When?**

without undue delay or within 72 hours

## ➤ **To who?**

Controllers, supervisory authorities and/or individuals affected

## ➤ **Why?**

Likelihood of risk/high risk to individuals but not if unlikely to cause harm i.e. encrypted data breaches



---

**New mandatory GDPR requirement dependent on type of processing and risk (unless public authority)**

**Do your core activities involve:**

- regular and systematic monitoring of individuals on a large scale?
- processing sensitive personal data on a large scale?

# GDPR: Higher penalties



## Heavy monetary sanctions

- for non-compliance up to **€20m (£15m)** or 4% turnover

## Increased powers

- for supervisory authorities and liaison with European Data Protection Board

## Claims by data subject claims

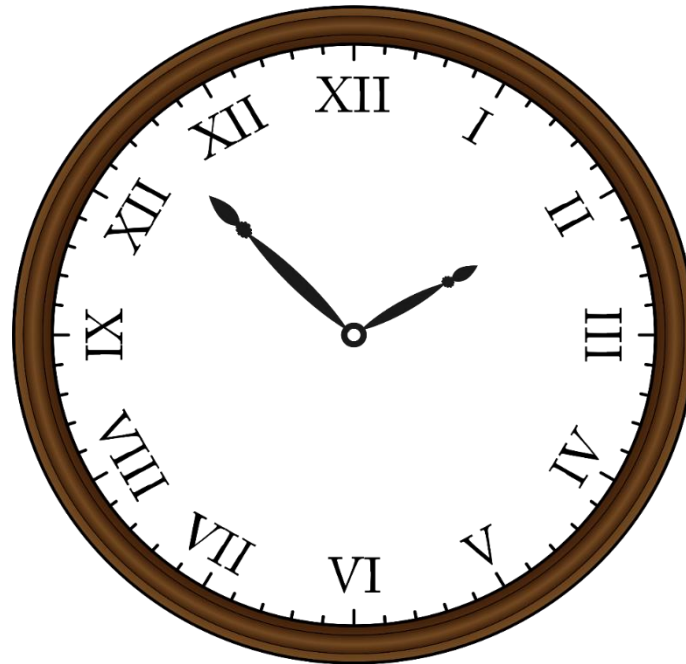
- for compensation for breaches

## “Class actions”

- by consumer associations

**Clock is ticking –  
it's time to get  
ready!**

---





**THANK YOU**

**[www.mrs.org.uk/standards](http://www.mrs.org.uk/standards)**