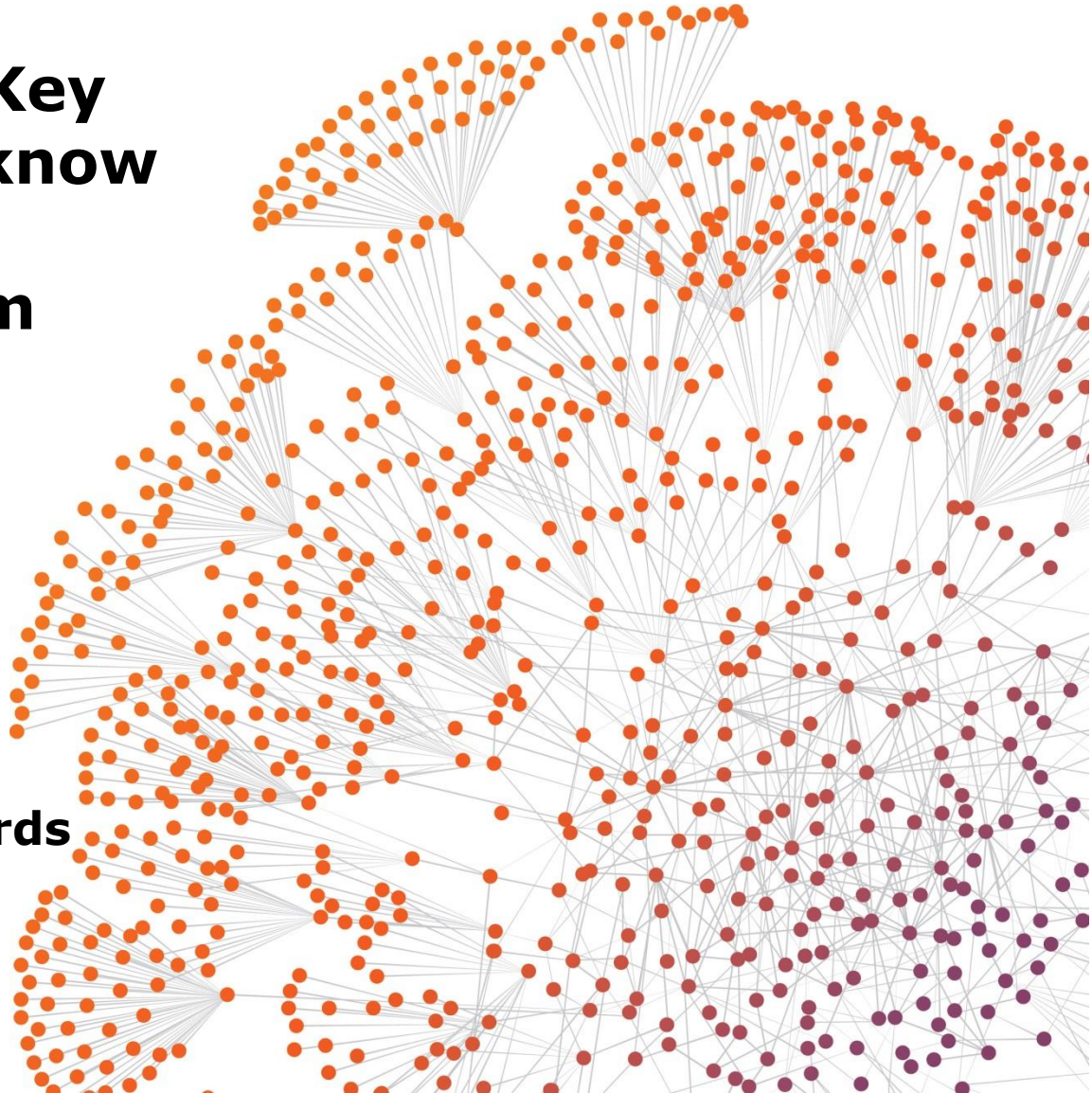
GDPR Countdown– Key things you need to know

IQCS Working Forum

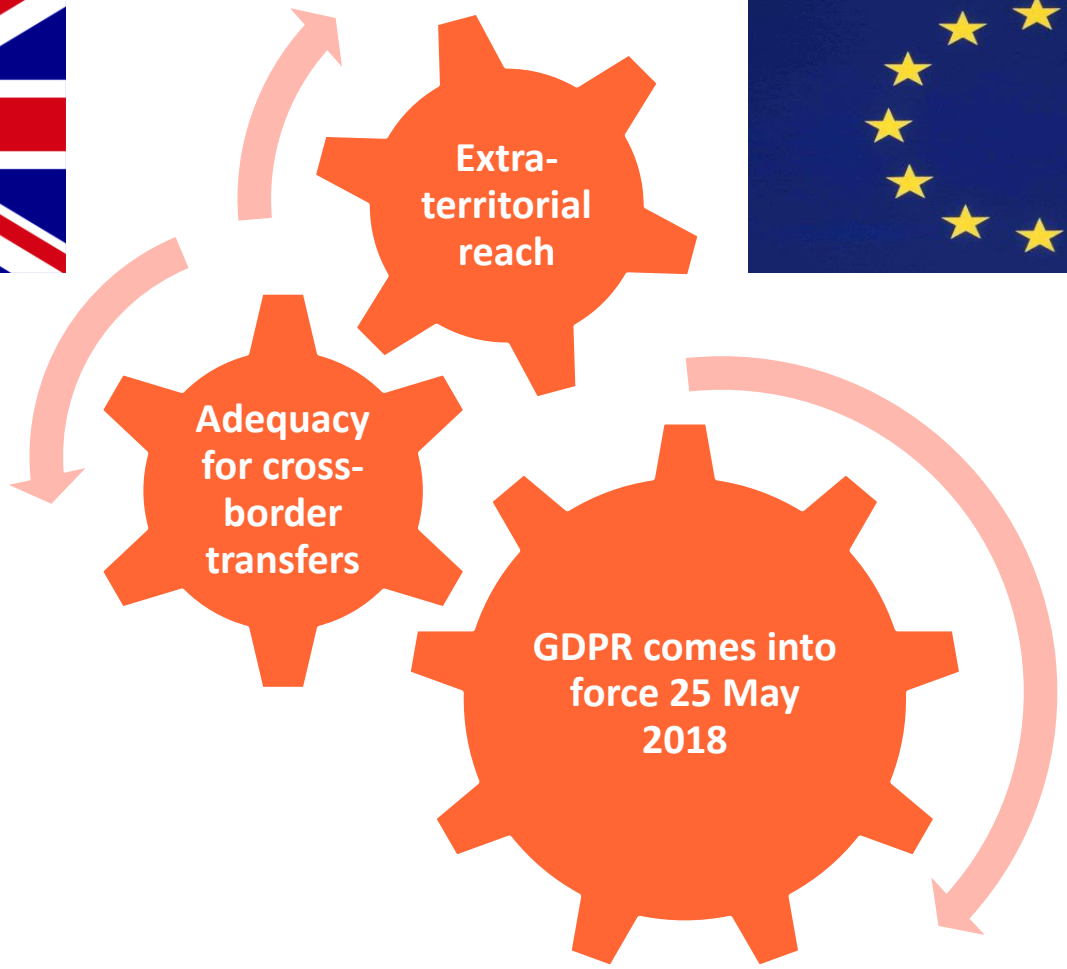
25th May 2017

Dr Michelle Goddard
Director of Policy & Standards

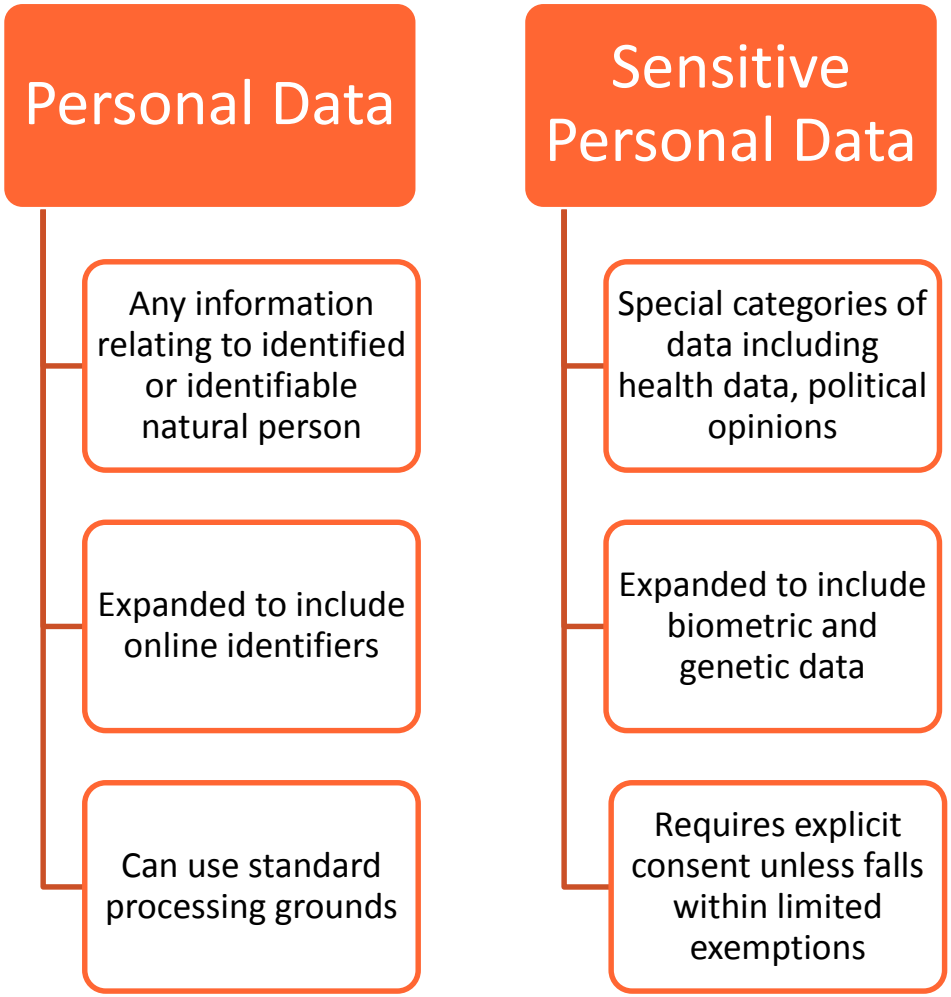


GDPR: New harmonised framework across EU

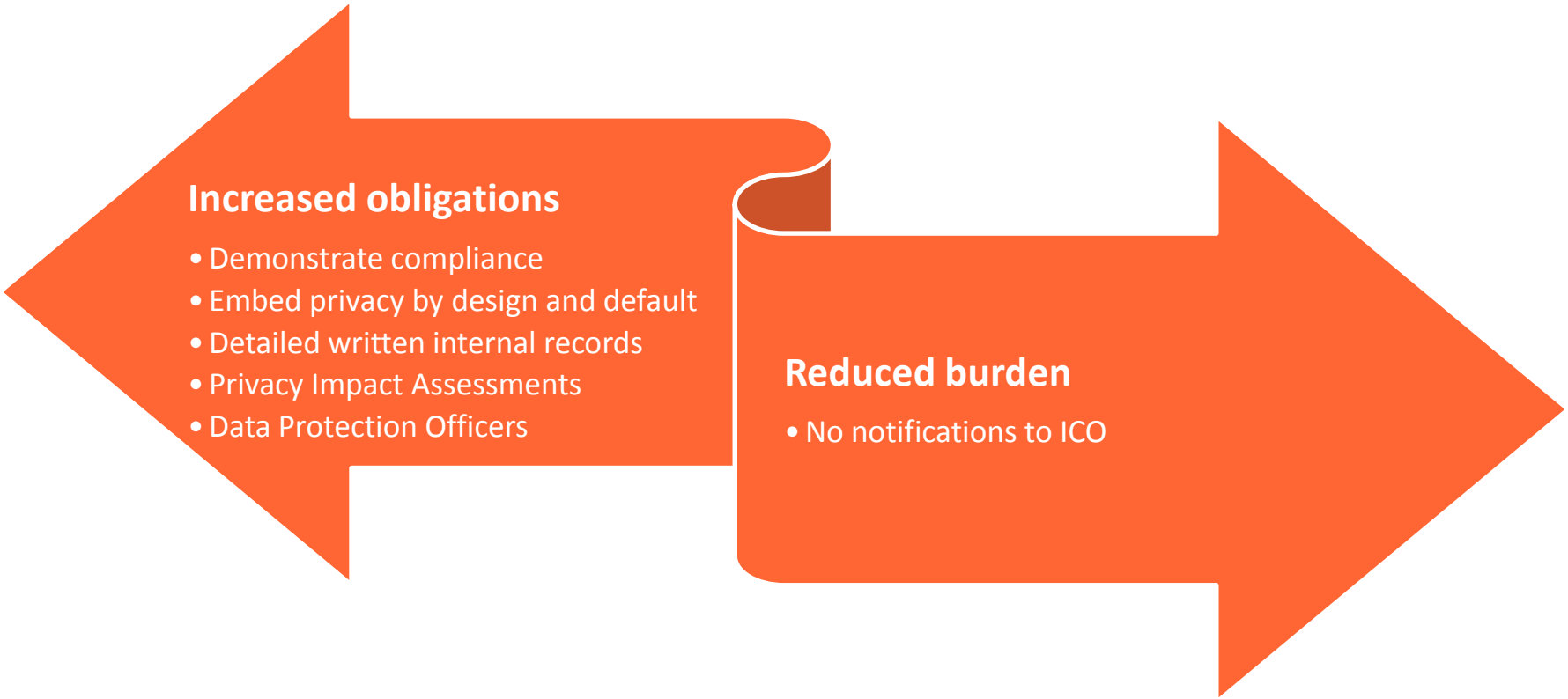
…. but what about Brexit?



GDPR: Wider scope of data categories



GDPR: Greater business accountability even for small buisinesses



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

GDPR: Data Protection Officer

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

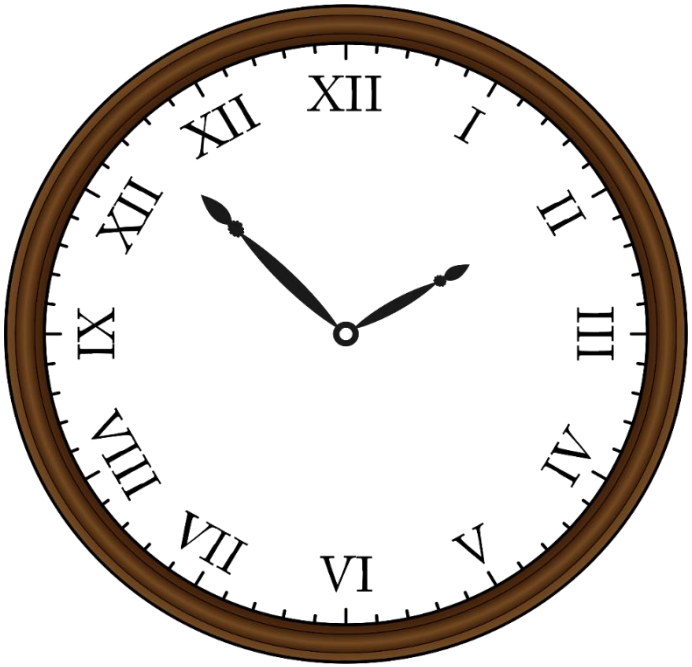
Do your core activities involve:

- 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