Your World First

Impact of the General Data Protection Regulation (GDPR) for ID systems and operators internationally

Key Issues review

UNCTAD e-commerce week April 2018

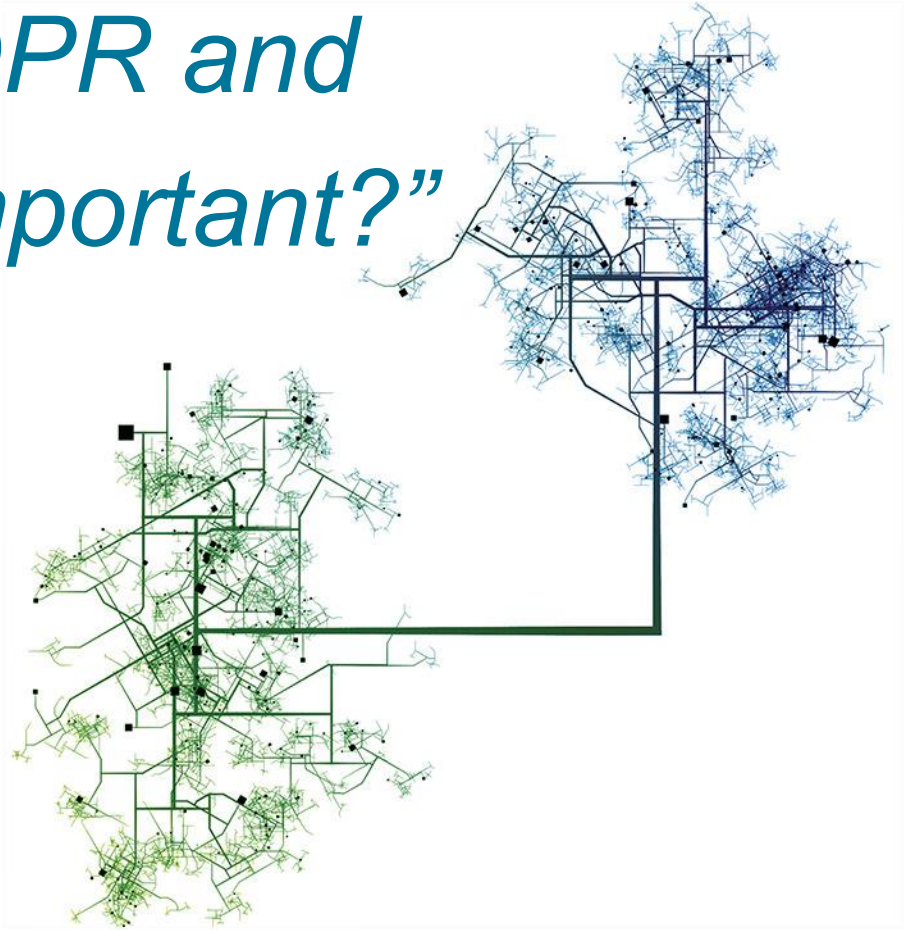
Chris Watson
Global Head of TMS
CMS LLP

Introduction and overview

- What is GDPR

- Key Questions for ID systems and operators
- What if we don’t comply?
- Effects on institutions?
- What about design of systems?
- GDPR Toolkit

"What is GDPR and why is it so important?"



General Data Protection Regulation (GDPR)

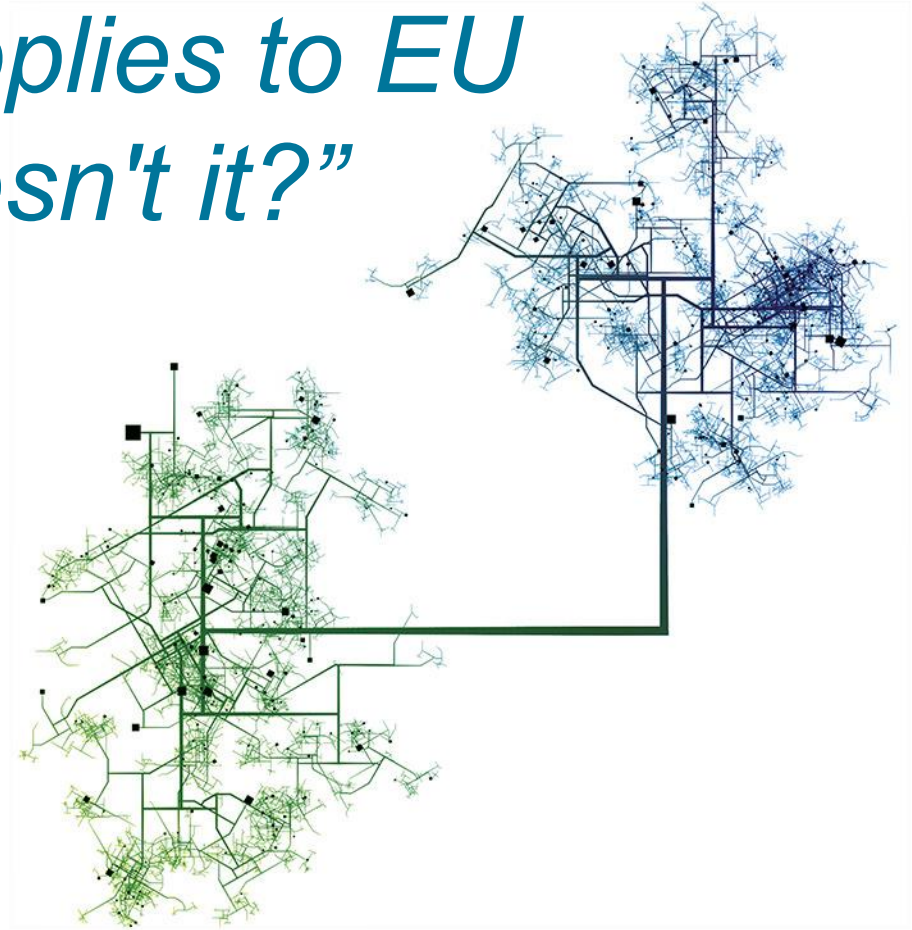
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
- Applies to all Member States from 25 May 2018
- Directly effective – replaces EU Directive and local implementing legislation
- Follows spirit and principles of the current legislation but imposes extensive additional new obligations including:
  - Obligations for data processors
  - Data subject rights
  - Anti-trust style fines

“Non-EU companies, or businesses that process EU personal data outside the EU, don’t need to worry about European data protection law do they?”

Key Questions for ID systems and operators- geography

- Extra-territorial effect
  - *the offering of goods or services (free of charge or paid for) to individuals in the EU; or*
  - *the monitoring of the behaviour of individuals in the EU.*
- Significant impact for Companies– international customer base

“But this only applies to EU Citizens doesn't it?”



Key Questions for ID systems and operators- who does it affect?

- The GDPR applies to “data subjects in the Union” (not EU citizens, nor residents even)
- The only requirement is that an individual must be in the EU for a period of time.
- The GDPR does not put a time limit on what that period should be and includes no exceptions or exemptions for people in transit.

"Do the GDPR changes really affect our industry outside the EU?

We don't really handle that much individual data?"

Key Questions for ID systems and operators- GDPR is pervasive across industries

- Yes; it affects all industries and bodies including governments and administrations
- Think about your use of personal data:
  - Customer data
  - Loyalty scheme/card scheme/ membership scheme data
  - Data transfers between your internal organisations
  - International transfers – outside of the UAE (to countries outside the EEA)
  - Staff HR data
- Controller or processor?
- Territorial scope

"What about Data transfers – does GDPR affect how we do these internally/externally?"

Key Questions for ID systems and operators- how does it apply to cross-border transfers and processing

International Transfers

- General rule is that for data transfers outside EU, there needs to be:
  - an adequate level of protection
  - appropriate safeguards put in place

Key actions:

- Put in place appropriate data transfer agreements, including EU Model Clauses, BCRs or other approved mechanism
- Your organisation should review and map key international data flows and assess whether systems and processes will continue to be appropriate
- Ensure processor contracts include protections against unauthorised transfers and sub-processing without consent

“It looks like GDPR could even apply to us and hat we do. What do we do next?”

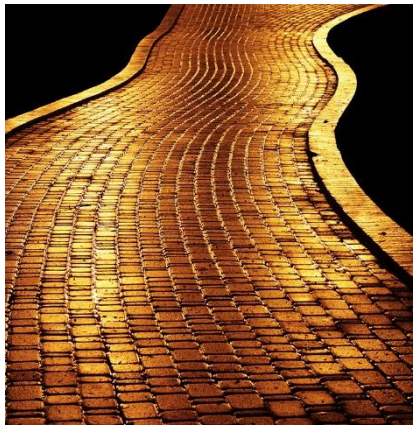
Key Questions for ID systems and operators – Road Map

Key Components

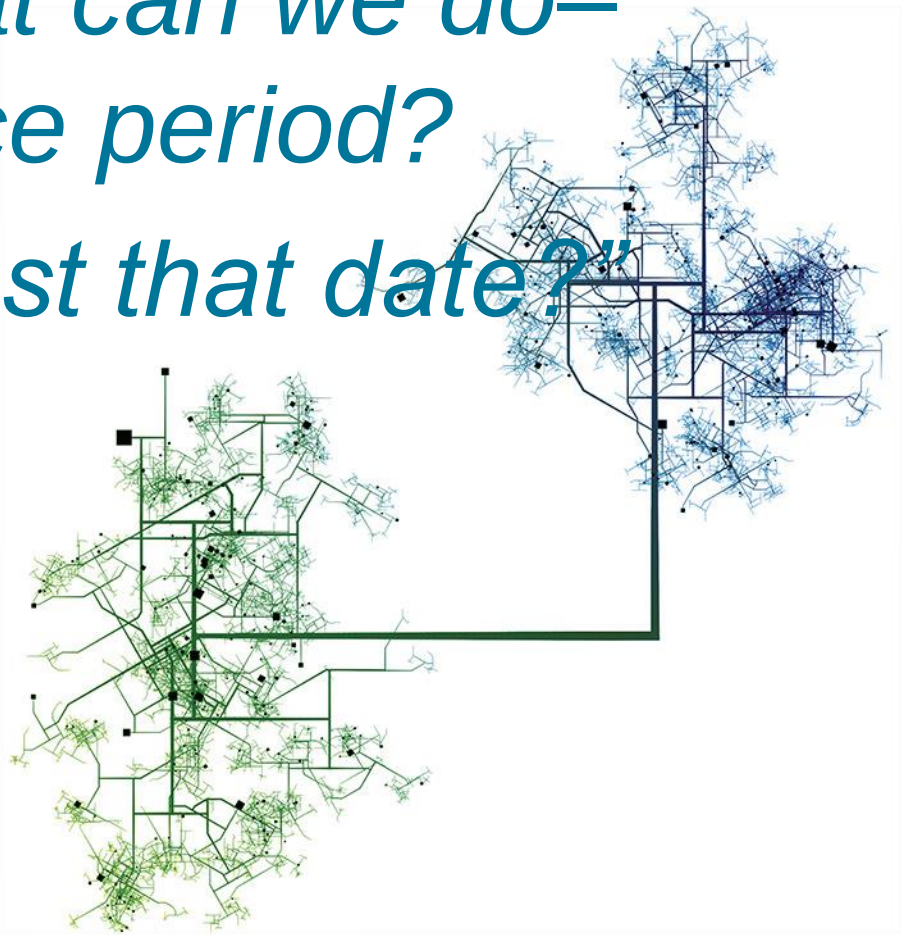
- comply with the data protection principles (Article 5)
- ensure you establish a legal basis in accordance with which personal data can be lawfully processed (*Article 6*), and
- avoid processing "special categories of personal data" (**sensitive data**) unless one or more of certain exceptional grounds can be shown (*Article 9*).

Considerations:

- appointing an EU representative
- appointing a data protection officer (DPO)
- keeping detailed data processing records

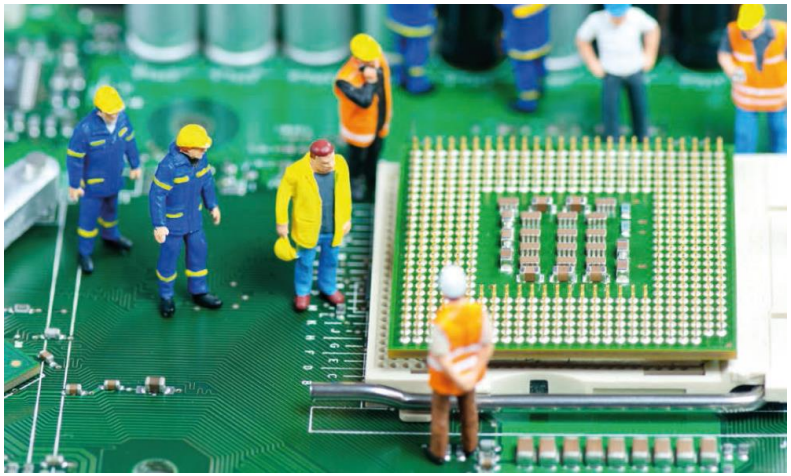


"If this all comes into effect from 25 May 2018 what can we do– is there a grace period? What happens post that date?"



Key Questions for ID systems and operators - the GDPR Timeline

- Two year implementation period ends on 25 May 2018.
- No grace period.
- Arrange tasks accordingly:
  - Immediate priority
  - Next priority
  - By GDPR Day 1
  - Ongoing



“What if we are found not to be in compliance?”

Key Questions for ID systems and operators – consequences of non-compliance

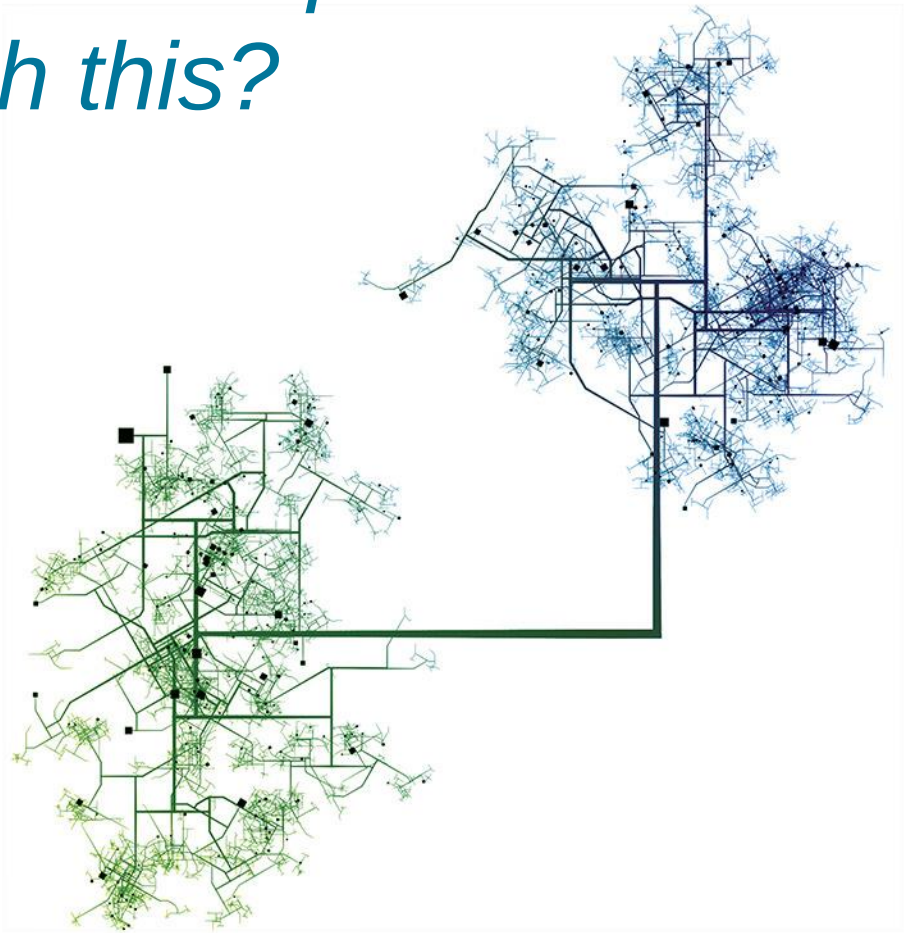
Fines & Enforcement

The GDPR implements significant fines for non-compliance

You could be looking at handing over up to:

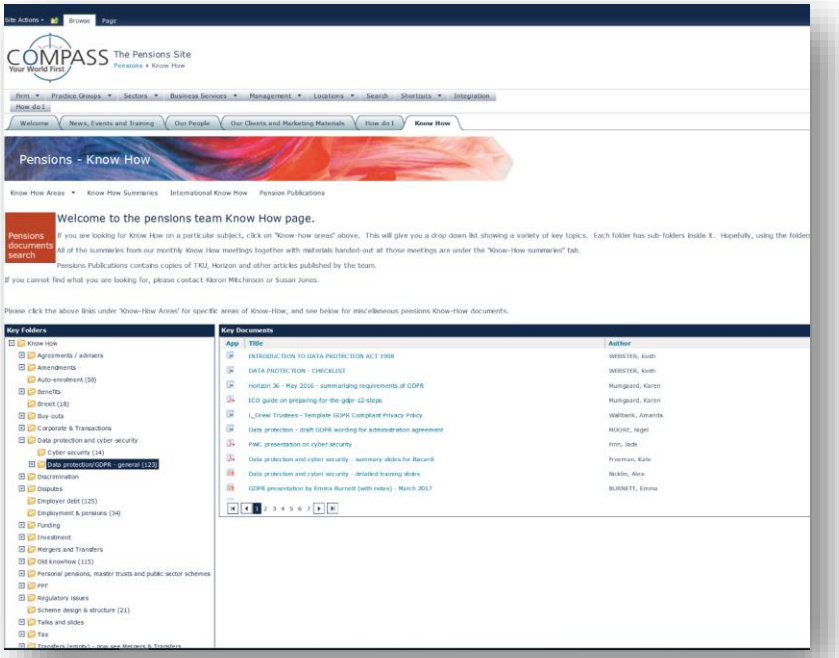
- 20 million EUR or 4% total worldwide annual turnover
- 10 million EUR or 2% total worldwide annual turnover

“Can’t somebody in IT/Compliance just deal with this?



Key Documents

- GDPR Project Timetable
- Long form/short form questionnaire
- Data Mapping Table
- Lawfulness of processing advice
- Privacy Notice
- Data Protection Policy
- Data Security Breach Notification Policy
- Third party contracts
- Scheme forms



Speaker today

Chris Watson
Global Head of TMC
CMS
E: chris.Watson@cms-cmno.com
T: +44 7768 377 443

C/M/S/ Law-Now™

Law.Tax

Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
www.cms-lawnow.com

C/M/S/ e-guides

Law.Tax

Your expert legal publications online.

In-depth international legal research
and insights that can be personalised.
eguides.cmslegal.com