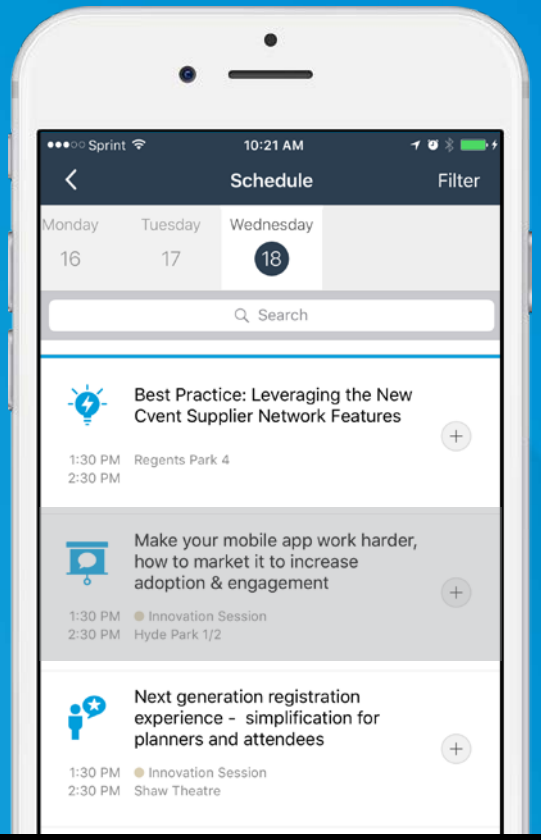
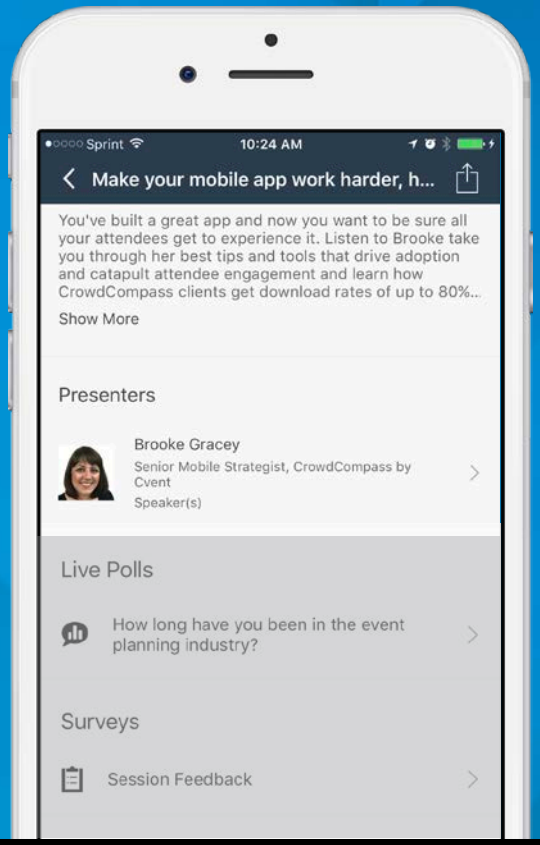
Download and Login to the Cvent CONNECT Europe Mobile Event App

Tap
On Schedule

Find
Your Session



Access Polls
and Live Q&A



More information at cventconnect.com/europe/mobileapp

Cvent CONNECT Europe

General Data Protection Regulation (GDPR): Do you understand it and are you ready?

Debrah Harding
Managing Director
MRS

Topics for today

Overview

10 Key elements of the General Data Protection Regulation (GDPR)

10 activities for preparing for GDPR

Discussion and Questions

Some context

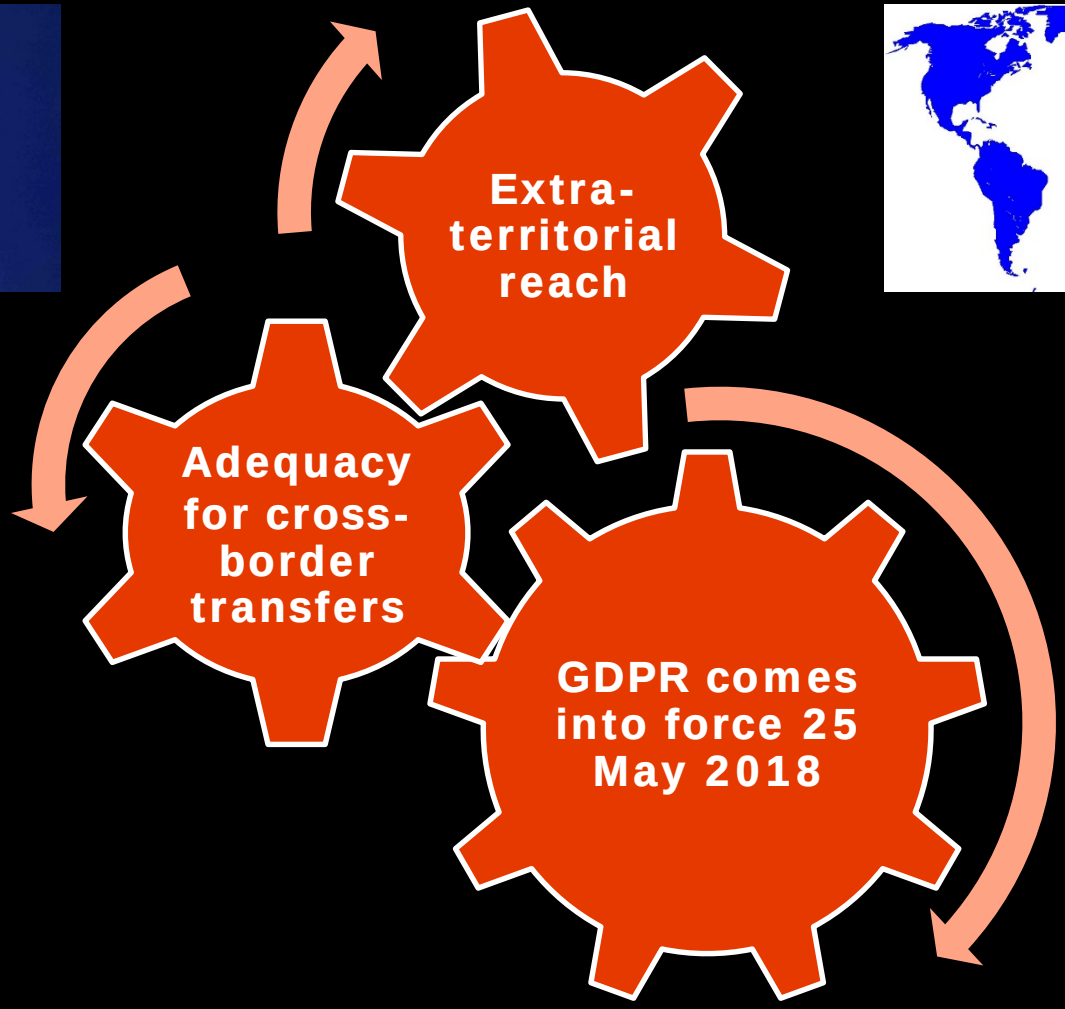
- **25th May 2018**

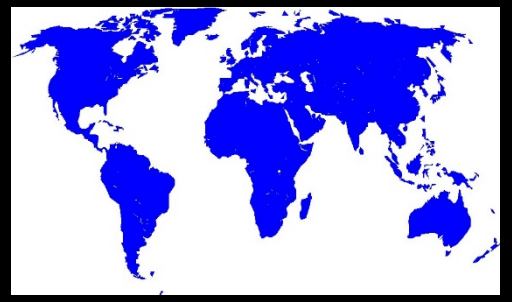
- Evolutionary not revolutionary:

  Fairness, transparency, accuracy, security, minimisation and respect for individuals all remain from current legislation

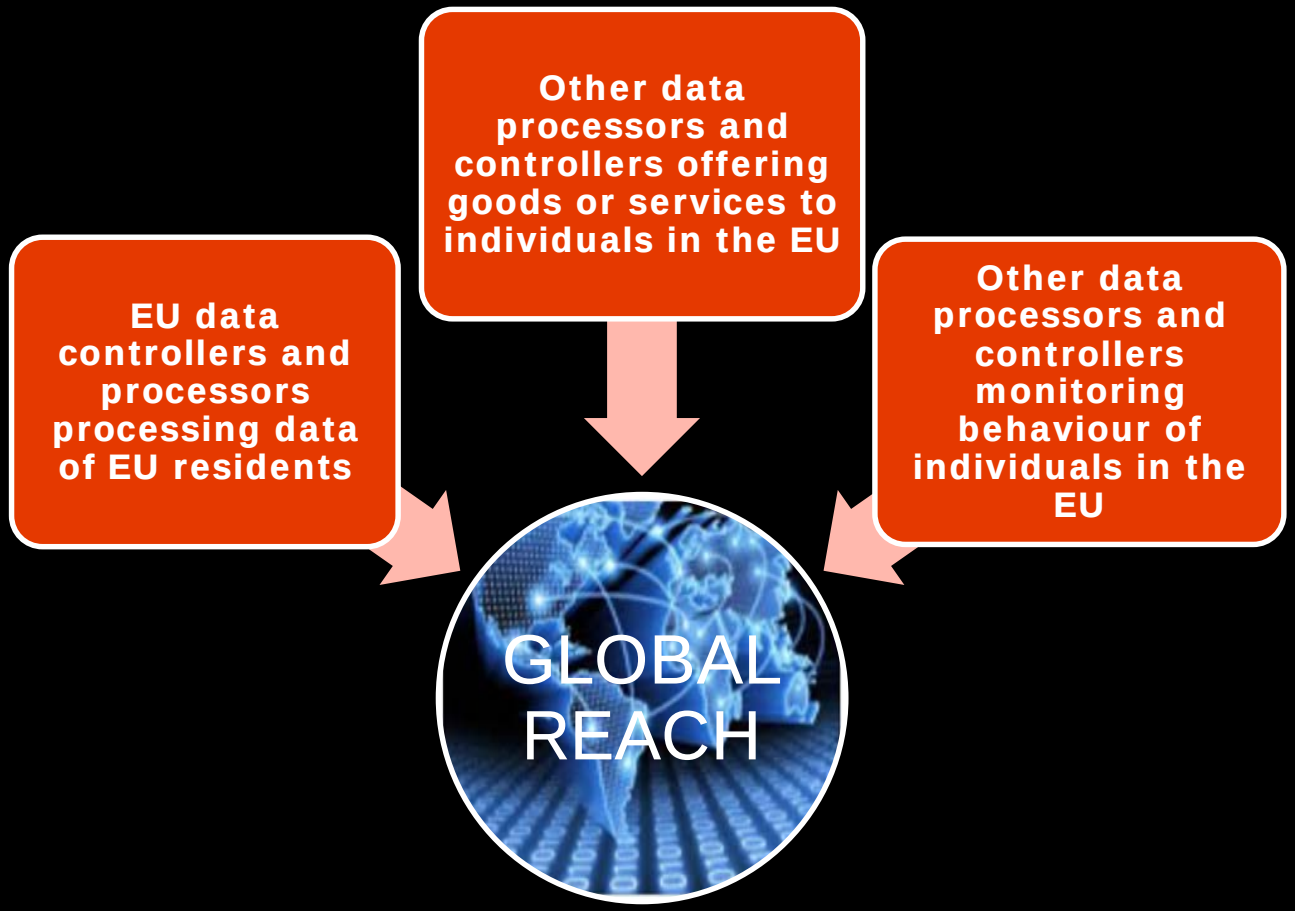
- Strengthened individual rights
- Increased business accountability
- Embedded privacy-centric focus

Element 1: Extra territorial reach





Element 1: Extraterritorial Reach



Element 2: Regulation v. national law

- Current privacy framework is a Directive:

  Each EU state has own law and own interpretation

- GDPR is a directly applicable Regulation:

  ...but Member States **can legislate on specific areas** including employment and **research**

Element 3: Privacy by design & default

- Philosophical approach:

  Privacy is a fundamental human right

- Privacy by design and default is core to GDPR:

  Supported on one side by **transparency** and the other by **accountability**

Element 4: Definition Of personal data

- Definition of personal data has been expanded:

  Data from which a living individual is **identifiable (by anyone) directly or indirectly**

- Online data which may be personal:

  Online identifiers, device identifiers, cookies IDs and IP identifiers

- Special categories of data (sensitive data):

  Current classes of data retained and extended to cover **genetic and biometric data**

Element 5: Children

- Children:

  Children **under 13 can never, themselves, give consent** to the processing of their personal data in relation to online services

  For children between **13 and 15 (inclusive)** the general rules is that parental consent must be obtained unless Member States legislate to reduce the age threshold

  Children aged 16 and over may give consent for the processing of their personal data

Element 6: Consent

Consent: freely give, specific, informed and unambiguous…by a clear statement or by a clear affirmative action signifying agreement to processing…

Have the right to **withdraw consent** at any time

Presumption that consent will not be valid unless **separate consents** are obtained **for different processing activities**

Forced or “omnibus” **consent** mechanisms **will not be valid** – no pre-ticked boxes or inactivity implying consent

Explicit consent for sensitive data

Element 7: Processing using other grounds

- Necessary for…

  the performance of a contract

  compliance with a legal obligation

  protect the vital interests of data subject

  performance of tasks in the public interest

  purposes of legitimate interests

Element 8: Further processing

- New processing purposes are compatible with original data processing purposes. Where processing is not based upon consent should take account of the following:

  Link between original and proposed purpose

  Context in which data has been collected

  The nature of the data

  The consequences of the proposed processing

  The existence of safeguards (including pseudonymisation)

Element 9: Data minimisation & pseudonymisation

- Data minimisation:

  Personal data must be adequate, relevant and limited

- Pseudonymisation:

  Personal data that has been processed so that it can no longer be attributed to a specific data subject without the use of additional information

Element 10: Enhanced rights and fines

- The current individual rights remain – right to know about processing, access, provided with supplemental information about processing. Plus new and enhanced rights:

  Right to be forgotten

  Right to request the porting of data to a new organisation

  Right to object to certain processing activities

  Right to object to decisions taken by automated means

Element 10: Enhanced rights and fines

- Fines may be imposed instead of, or in addition to, measures that may be ordered by supervisory authorities. There are two tiers of administrative fines:

  - Some contraventions will be subject to administrative fines of up to €10,000,000 or, 2% of global turnover, whichever is the higher

  - Others will be subject to administrative fines of up to €20,000,000 or 4% of global turnover, whichever is the higher

- Higher fines for breaches of basic principles including consent conditions, data subject rights, transfers and non-compliance with orders by supervisory authorities

10 Next Steps: Step 1

1. Determine whether GDPR affects your organisation

   Are you or your organisation a Data Controller?

   A Data Processor?

   Both?

10 Next Steps: Step 2

2.Conduct an organisational information audit including all subcontractors relating to the data supply chain. Some questions to consider…

Where is personal data stored?

Who has control and access to personal data?

Is personal data shared with third parties?

Is personal data shared with other processors?

Are your subcontractor arrangements sufficient?
What about your subcontractors' subcontractors?

10 Next Steps: Step 3

3. Understand the legal grounds for collecting data

Do you collect data using consent?

If you use consent – look at notices, policies - to ensure you are being fair and transparent about processing

10 Next Steps: Step 3

3. Understand the legal grounds for collecting data. Fair processing notices, some things to consider:

Written clearly in an accessible manner

Layered & tailored to communication platforms
- condensed overview
- link to full policy
- direct to website if using other means

Include for example: identity, contact details, legal basis for processing, recipients of data, transfers, retention, right to access

10 Next Steps: Step 4

4. Review and strengthen your IT arrangements

Can your IT systems and processes cope with the new rights including right to be forgotten, data portability?

What security measures are in place? Are these sufficient?

Who has access to personal data? Within your organisation? Outside of your organisation and staff?

What arrangements are in place to manage data retention and destruction?

10 Next Steps: Step 5

5.Review your policies, processes and training

Do staff understand the new obligations?

Have all staff had appropriate training for their data responsibilities?

What arrangements are in place for freelancers, casual workers, etc?

What happens when role's change? Is top-up training given?

What about subcontractors?

10 Next Steps: Step 6

6.Determine if you need a Data Protection Officer (DPO)

Must appoint a DPO if...

a) core activities require regular and systematic monitoring of data subjects on a large scale; and/or
b) large scale processing of sensitive data

DPOs must be:
- autonomous
- well resourced
- report to a senior level
- have high job security (if employed)
- necessary level of legal/data expertise based upon processing undertaken

10 Next Steps: Step 7

7. Build a comprehensive GDPR implementation and compliance programme

Start GDPR implementation NOW if not started

Clear set of activities, priorities, timings with resource allocated

10 Next Steps: Step 8

8.Prioritise on areas with highest risks and impact

Think about high risk data processing within your business

Consider those activities with the higher fines attached – sensitive data, consent, subject access rights, etc

10 Next Steps: Step 9

9.Instigate and conduct Privacy Impact Assessments/ Data Protection Impact Assessments

This is one way to ensure that Privacy by Design becomes embedded into your corporate culture

Assessments can include:
- a description of envisaged data processing
- assessment of the need for processing
- assessment of the risks to data subjects
- measures to mitigate risks
- steps to ensure GDPR compliance

10 Next Steps: Step 10

10. Prepare for data breach notifications

Set up internal procedures including:
- breach notifications
- monitoring to enable detection of breaches
- breach reporting lines

Discussion & Questions

Don’t forget to take the session survey!