APRC Conference 2017

The 20 Million Data Question: an Update on the NEW European Data Privacy Laws

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

Questions

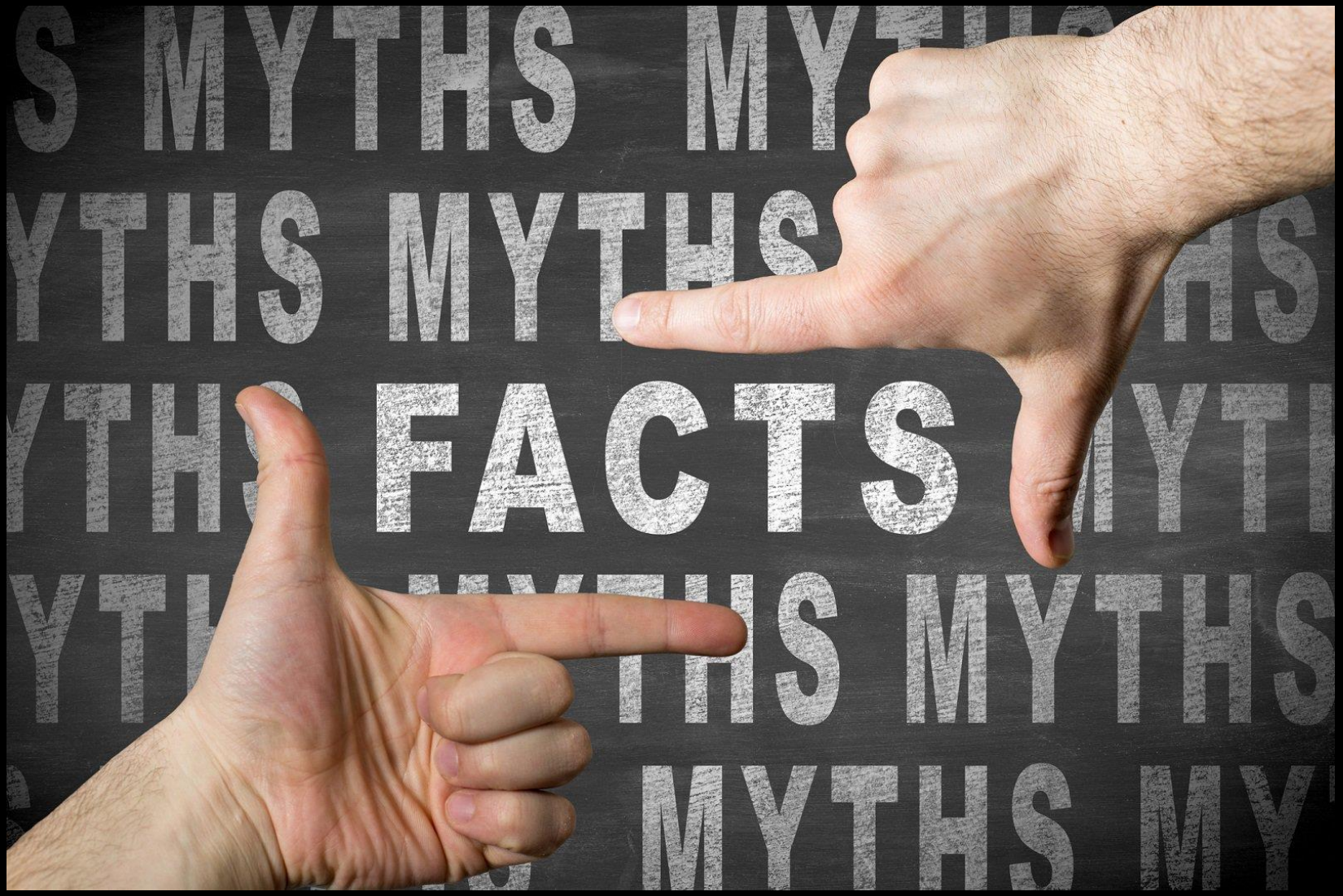
Some context

- 25th May 2018

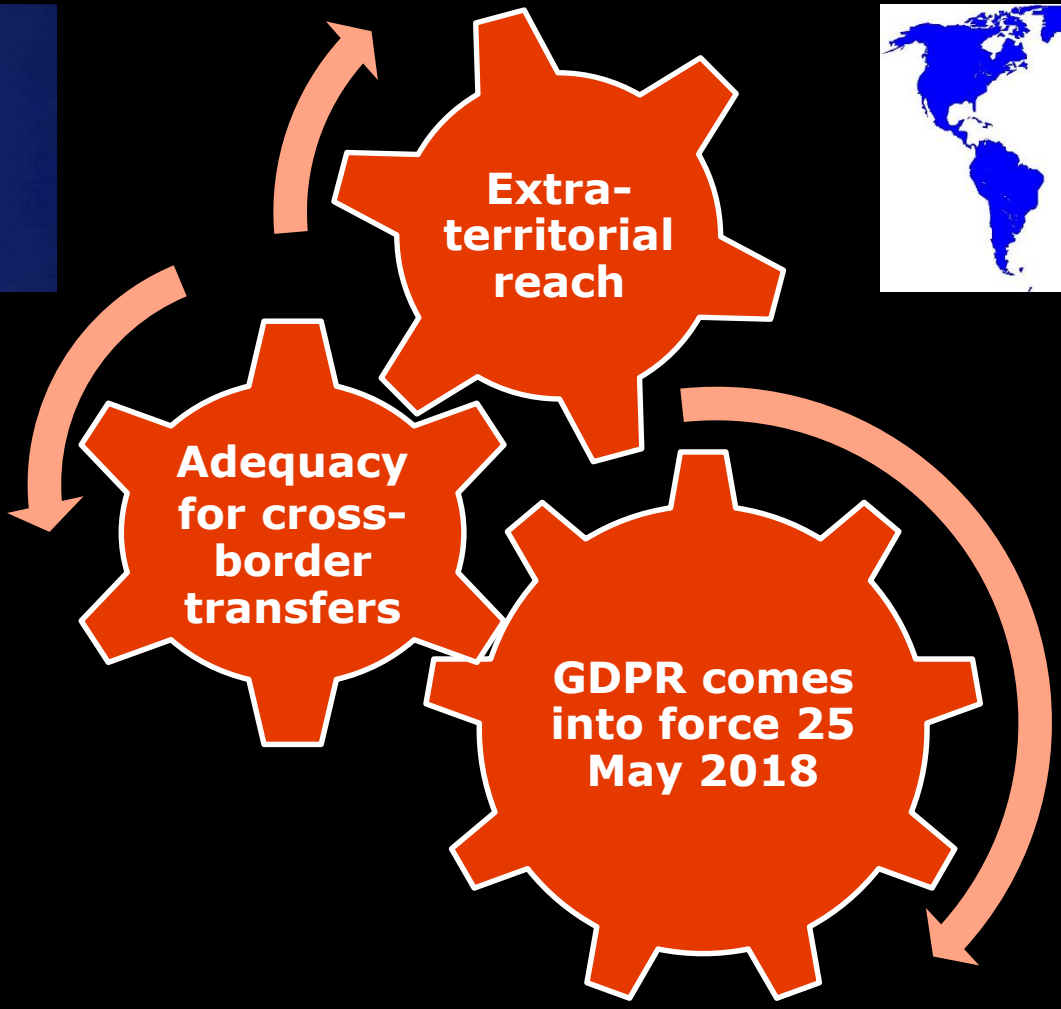
- Evolutionary not revolutionary:

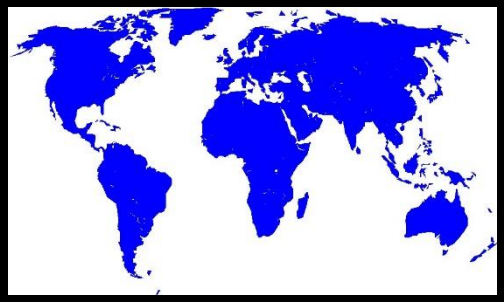
  Fairness, transparency, accuracy, security, minimisation and respect for individuals all remain from current legislation

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


MYTHS
FACTS
MYTHS

Element 1: Extra territorial 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 Regulation adopted by Member States

  …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:

  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:

  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, plus some are enhanced. Rights include:

  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

10 Next Steps

1. Determine whether GDPR affects your organisation

It is does…

2. Conduct an information audit inc. subcontractors
3. Understand the legal grounds for collecting data
4. Review and strengthen your IT arrangements
5. Review your policies, processes and training
6. Determine if you need a Data Protection Officer
7. Build a comprehensive privacy compliance structure
8. Prioritise on areas with highest risks and impact
9. Instigate and conduct Privacy Impact Assessments
10. Prepare for data breach notifications

GDPR: Ongoing initiatives

GDPR Code of Conduct (EFAMRO/ESOMAR)

Research Exemption Lobbying (MRS/EFAMRO/ESOMAR)

Legitimate Interests WG (MRS/IAF)	Legitimate Interests WG (MRS/DPN)	Regulatory Guidance 3 MRS Guides issued so far Consultations (MRS/EFAMRO/ /A29WP)

Any questions?