Jisc

24/06/2016

What will the GDPR do for us?

Andrew Cormack (@Janet_LegReg)

What is it?

General Data Protection Regulation, passed 2016, in force May 2018

Replaces 1995 Data Protection Directive

» 88 pages replacing 20 ☹

"Regulation" should mean less variation between countries

» But still lots of definitions/derogations/enforcement variety possible

What does it do?

More principles, fewer tickboxes

» E.g. "Privacy by default and by design"

» But "accountability" still seems to require a lot of documentation

"Consent" moves closer to traditional English law meaning, so more restricted

» Need to look at other justifications for processing too

» Not "everything by consent" ☺

Some new rights for individuals (e.g. portability, restriction, erasure)

» Little information yet on what these will mean in practice

Much bigger fines – designed to get management attention

What doesn't it do?

Resolve all the questions, e.g.

» One-stop-shop promise made to both data controllers and data subjects

» Says "risk-based" but still lots of binary obligations

Help with spying/export uncertainty

Get the Internet

» Physical location of data still key

» Clouds treated as data processing bureaux

What doesn't it do?

Resolve all the questions, e.g.

» One-stop-shop promise made to both data controllers and data subjects

» Says "risk-based" but still lots of binary obligations

Help with spying/export uncertainty

Get the Internet

» Physical location of data still key

» Clouds treated as data processing bureaux

BREAKING

EU Referendum Result…

BREAKING

EU Referendum Result…

Doesn't make a difference

Regulation applies to anyone processing Europeans' data

» If you want them as students/staff/customers, still need to comply

Legal challenges over compatibility of current UK law

» Might need to do more in future to demonstrate "equivalent protection"

General Issues

With thanks to the ICO…

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

1. **Awareness**
   You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2. **Information you hold**
   You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3. **Communicating privacy information**
   You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4. **Individuals' rights**
   You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5. **Subject access requests**
   You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6. **Legal basis for processing personal data**
   You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

7. **Consent**
   You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

8. **Children**
   You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

9. **Data breaches**
   You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10. **Data Protection by Design and Data Protection Impact Assessments**
    You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11. **Data Protection Officers**
    You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

12. **International**
    If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

ico.
Information Commissioner's Office

ico.org.uk

Particular Areas of Interest

- Cloud
- Federated Access Management
- Breach Notification
- Incident Response

Implications for Cloud

Claims global regulation of SaaS providers to EU consumers

Otherwise lots of uncertainties

» Status of PaaS/IaaS platforms? Data controller, data processor, something else?

» Obligations on any of them a poor fit for cloud model

» Need clarity: maybe from promised controller/processor guidance?

Location-dependency of law *vs* location-independency of cloud

» *Schrems* cases create uncertainty for all export methods (not just Safe Harbor)

» What about spying by EU states? Or remote spying? "Data localisation" now a thing

Irony: most clouds provide better physical/technical security than in-house

Implications for Federated Access Management

We got there first! R&E federations already do recognised good things:

- Pseudonyms
- Data (release) minimisation
- Purpose limitation
- Consent only for genuinely optional things

And now Regulation should provide

- Better harmonisation of "legitimate interests" justification & rules (within EU)
- Possibility of using same legal framework for services outside EEA

Implications for Breach Notification

Breach = unauthorised/accidental loss, alteration, disclosure or access to personal data

Document all breaches

Report to ICO unless unlikely to risk rights and freedoms of individuals

- Within 72 hours, or explain why
- Nature of breach, categories and numbers of records and individuals affected
- Mitigation measures taken/proposed

Report to individuals if high risk to rights and freedoms of individuals

- Unless already mitigated (e.g. by encryption)
- Can take ICO's advice on notification

Seems to be "learn to make things better" motive, rather than "name and shame" ☺

Implications for Incident Response

"ensuring network and information security" recognised as a legitimate interest (Rec.49)

e.g. "preventing unauthorised access … malicious code distribution … stopping 'denial of service' attacks and damage to computer and electronic communication systems"

So processing personal data allowed, subject to balance of interests test

- Which normal CSIRT activities seem to satisfy
- Academic paper on this about to be submitted

Again, can (probably) use same legal framework for international collaboration

Think…

Data Protection, not Privacy

Risk, not Compliance

What guidance are regulators providing

Watch these spaces…

ICO:

» https://ico.org.uk/for-organisations/data-protection-reform/

» https://ico.org.uk/for-organisations/data-protection-reform/guidance-what-to-expect-and-when/

Regulation:

» http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC

Me:

» https://community.jisc.ac.uk/blogs/regulatory-developments/tags/Data-Protection-Regulation

Thanks

Andrew Cormack
Chief Regulatory Adviser, Jisc Technologies

Andrew.Cormack@jisc.ac.uk

https://community.jisc.ac.uk/blogs/regulatory-developments/tags/Data-Protection-Regulation