22/09/2017

GDPR: Good news for information security

Andrew Cormack (@Janet_LegReg)

General Data Protection Regulation 2016/679

Regulates processing of Personal Data (widely defined)

- In force 25th May 2018
- Still waiting for DPA guidance, national choices, …

New accountability principle

- What personal data are you processing? (old DP Directive)
- Why are you processing this personal data? (new DP Regulation)

New rules to

- Reduce over-use of consent – examine other legal bases
- Increase information & rights for individuals

GDPR supports reactive and proactive infosec

Breach Notification

Unauthorised/accidental loss, alteration, disclosure or access to personal data

All breaches	• Document
Risk to rights/freedoms	• Report to Data Protection Authority (72 hour expectation) • Nature; Number/type of records/people affected; Mitigations
High risk to rights/freedoms	• Also notify individuals (unless mitigated) • Can take Data Protection Authority advice

Security & Incident Response

"ensuring network and information security … CSIRTs… providers of networks and services… " (Rec.49)

A legitimate interest… (for processing personal data)

If necessary/proportionate…

Balance of interests test…

Very like security good practice (see paper)

Technologies etc. mentioned

Encryption	• Mitigate breaches
Pseudonyms	• Reduce risk
Authorisation	• Assist compliance
Exercises	• Test readiness

Data Protection by Design

New Incentives

- Security/Incident Response clearly lawful
- Draft ePrivacy Regulation also recognises patching etc.
- Increased public awareness
- Much bigger fines (€20M/4%)
- Damages, not just for monetary loss

Opportunities to improve

- Regulator guidance
- Lessons learned from breaches
- Compare public notifications with our practice
- NIS Directive => more sharing
- Cloud security standards etc.

Watch these spaces

- Regulators
  - http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 (EU)
  - https://ico.org.uk/for-organisations/data-protection-reform/ (UK)
- Regulation (2016/679/EU):
  - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
- Me:
  - https://community.jisc.ac.uk/blogs/regulatory-developments/tags/Data-Protection-Regulation
  - https://www.script-ed.org/?p=3180
  - GDPR webinar 31/10 https://eventr.geant.org/events/2731

Thanks

Andrew Cormack
Chief Regulatory Adviser, Jisc Technologies

Andrew.Cormack@jisc.ac.uk

One Castlepark Tower Hill Bristol BS2 0JA
T 020 3697 5800

customerservices@jisc.ac.uk
jisc.ac.uk