GDPR: Good news for information security

Andrew Cormack (@Janet_LegReg)
Regulates processing of Personal Data (widely defined)
- In force 25\textsuperscript{th} 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
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
“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)
<table>
<thead>
<tr>
<th>technologies mentioned</th>
<th>benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>• Mitigate breaches</td>
</tr>
<tr>
<td>Pseudonyms</td>
<td>• Reduce risk</td>
</tr>
<tr>
<td>Authorisation</td>
<td>• Assist compliance</td>
</tr>
<tr>
<td>Exercises</td>
<td>• Test readiness</td>
</tr>
</tbody>
</table>

**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

1. Regulator guidance
2. Lessons learned from breaches
3. Compare public notifications with our practice
4. NIS Directive => more sharing
5. Cloud security standards etc.
» 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):

» 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
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