24/04/2018

# Data Protection Impact Assessments

Andrew Cormack, Chief Regulatory Adviser (@Janet_LegReg)

# GDPR Art 35

DPIA required

35(1) "if likely to result in a high risk to the rights and freedoms of natural persons"

35(3) in particular, where

- systematic and extensive evaluation of personal aspects … based on automated processing … decisions … produce legal effects", or
- "processing on a large scale of special categories of data", or
- "systematic monitoring of a publicly accessible area on a large scale"

# Article 29 WP

## Nine factors…

Evaluation or scoring

Automated decision-making

Systematic monitoring

Sensitive (or highly personal) data

Data processed on large scale

Matching/combining datasets

Vulnerable data subjects

Innovative use or new technological/organisational solutions

Processing prevents data subject exercising right/using service/contract

Match 2 or more => usually need a DPIA

# Jisc Services that may reach this threshold

## Security Operations Centre

» Large scale

? Systematic monitoring

? Innovative use

? Automated decision-making

## Learning Analytics Service

» Large scale

» Matching/combining datasets

» Innovative Use

? Special category data (one day)

# Sources for how to do it…

Art29 (http://ec.europa.eu/newsroom/document.cfm?doc_id=47711)

» Threshold guidelines

» Required outputs (from which you can reverse engineer)

CNIL (https://www.cnil.fr/en/cnil-publishes-update-its-pia-guides)

» Lots of detail on risk sources (have we forgotten any?)

ICO (draft) (https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/data-protection-impact-assessments-dpias-guidance/)

» Too late, maybe next time ☹

» New criteria for mandatory and probable DPIAs ☹

# Or DIY...

# Data Gathering/Reporting

## Based on GDPR structure

Description of Operations and Purpose

- Controllers, processors, recipients, purpose/legal basis…
- What data, how, where, how long…

Assessment of Necessity and Proportionality

- Individual rights/principles fit here too

Assessment of Risks to Rights and Freedoms (see later)

Measures to Address Risks, and Demonstrate Compliance (see later)

Conclusions

- Are risks mitigated? Recommendations

# Risk Assessment (1)

## Art 29 suggestion

Look at risks to confidentiality, integrity, availability

Caused by internal, external, environmental sources

By accident or deliberately

# Risk Assessment (2)

## Because we don't have a 3D piece of paper…

Look at possible harms to

- Confidentiality
- Integrity
- Availability

Which would affect rights/freedoms?

Assess **impact** of each of these

# Controls/mitigation

What measures hinder those (significant) impacts being caused by

- Internal (accident/malicious)
- External (accident/malicious)
- Environment (accident)

Now what's the **likelihood**?

- Some may also reduce **impact**, e.g. redundant data centres

Anything else we need to/could do?

How to monitor compliance?

# Still working out…

# Third parties

SOC: only limited disclosures to other Data Controllers

- E.g. law enforcement (permitted by UK law)
- E.g. other CSIRTs etc. (data minimisation, then check LegInt)

Learning Analytics: Jisc as (mostly) data processor

- DPIA still required, but
- Some aspects depend on data controller
  - E.g. Subject rights, organisational security measures…
- And sub-processors: need to pass on obligations to them too

# Consultation/Feedback

UK ICO draft now stresses user consultation

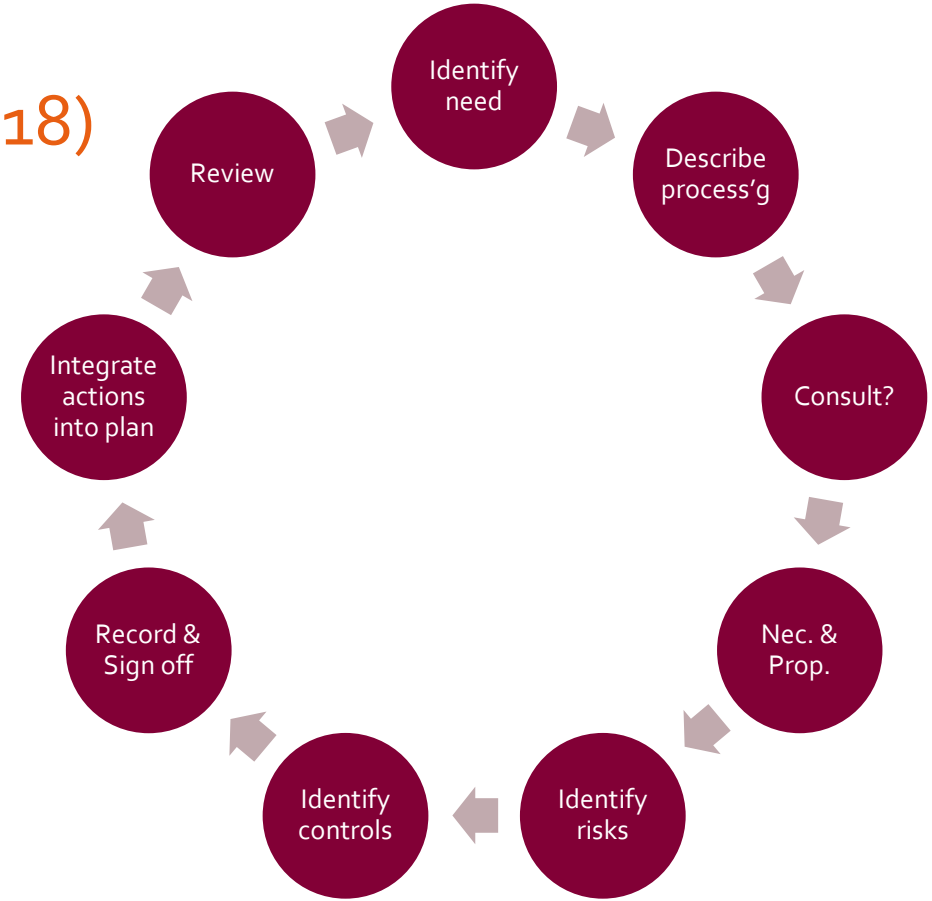
- Seems to suggest ***before*** own risk/mitigation assessment…
  - More efficient to ask users about issues you ***didn't*** spot?
- Consult on 1st DPIA report as part of 2nd?

And suggests a cyclic process

- As processing, risks, mitigations, knowledge etc. develop
- Repeat in 18 months or so?

In the meantime there may be internal functions to do…

# ICO draft (March 2018)



# 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