12/12/2018

Explorations in the GDPR

Andrew Cormack, Chief Regulatory Adviser (@Janet_LegReg)

Route Map: in search of harmony

And opportunities to create it…

What is a University?

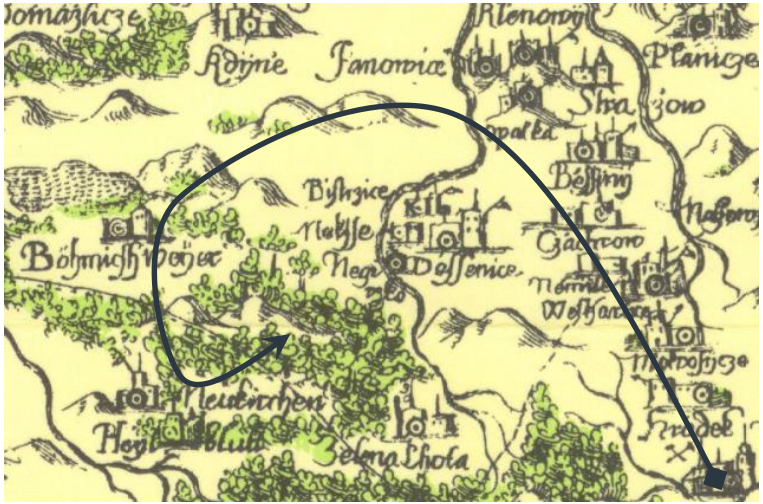
Network & Information Security

Research

Learning Analytics

Intelligent Campus

Well-being



What is a University?

UK, DK, maybe others: a "Public Authority"

» So using "Public Interest" as justification

Other MS: just another data controller

» So using "Legitimate Interest" as justification

Disharmony? Maybe not…

» GDPR text pretty much identical for "PubInt" & "LegInt"

» Just missing the balancing test against data subject rights and freedoms…

» Do that test anyway => Harmony in practice if not in terminology

NB: GDPR Rec.43 presumes consent to a Public Authority is not free…

Network & Information Security

Explicitly covered by Rec.49

- But some odd interpretations out there
- No, you don't need hackers' consent to log & investigate them…

Rec.49 says Legitimate Interest ***even*** for public authorities

- Write privacy-respecting incident detection/response processes
- Assess rights balance
- Implement appropriate collection, analysis, retention

Good compatibility with existing CSIRT practice, including info.sharing

Cormack AN (2016), 13(3) SCRIPTed 258-282 "Incident Response: Protecting Individual Rights…"

Research

Disharmony by design ☹

- GDPR only sets high-level framework
- Each Member State decides detailed rules and when they apply

Confusing terminology

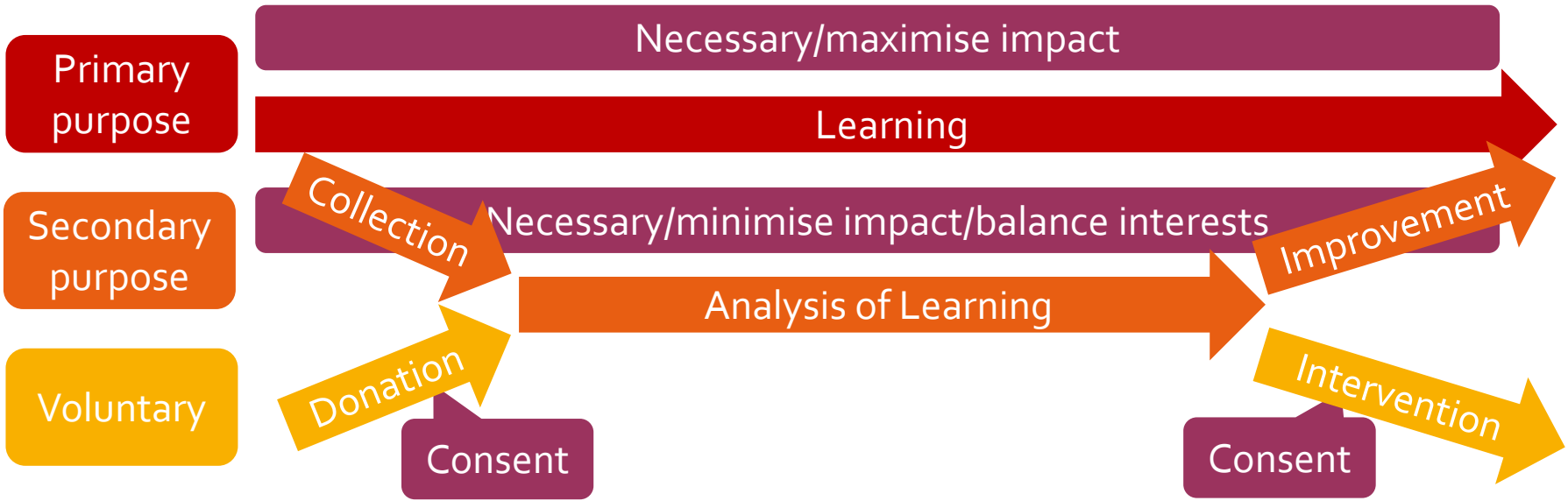
- Research "consent" not the same as GDPR "consent"
- Research "personal data" may not be same as GDPR, either

But research ethics process should look a lot like a DPIA

- May well be doing right-ish things already
- Main challenge probably to find all research using personal data

Learning Analytics (visualisation 1)

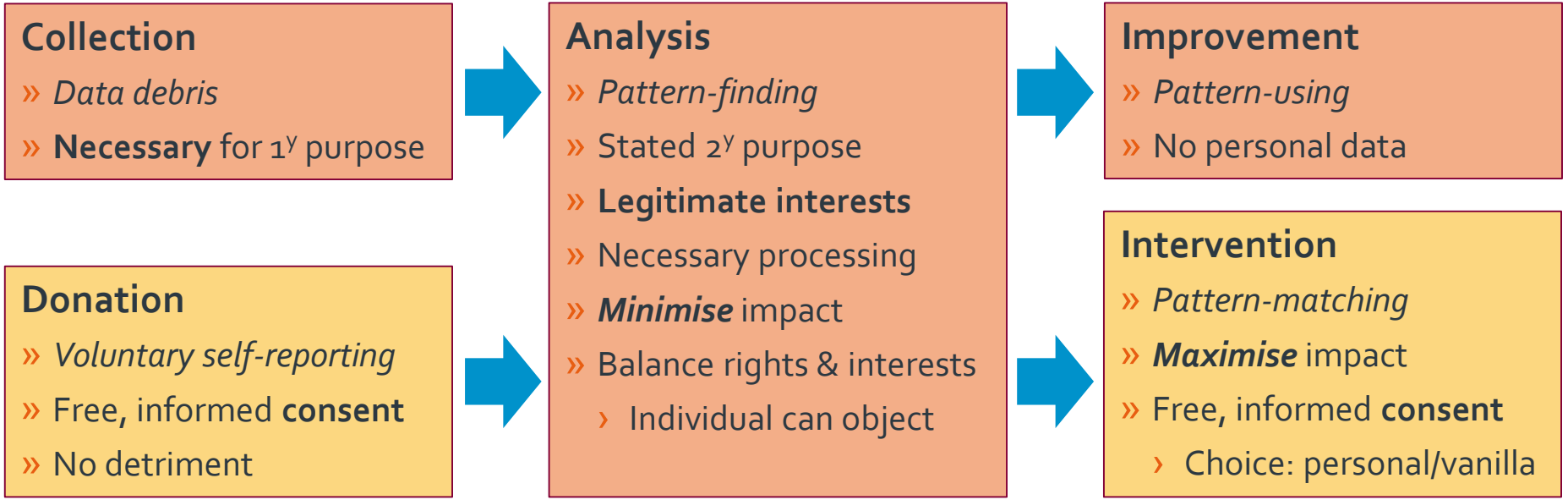
Compatible purpose + Voluntary participation



Cormack AN (2016), 3(1) Journal of Learning Analytics 91-106 "A Data Protection Framework for Learning Analytics"

Learning Analytics (visualisation 2)

A responsible way to use big data techniques



Cormack AN (2016), 1(1) Journal of Information Rights, Policy and Practice "Downstream Consent…"

Intelligent Campus

Senses and Risks (based on Art29 RFID DPIA)

	Vision	Hearing	Location
0: Presence	Motion detection	Sound level	
1: Counting			Queue measuring
2: Identifying	CCTV monitoring		Location-aware app
3: Recording	CCTV recording	Audio recording	Access card/logs
4: Analysing	Face recognition	Trigger words	Behaviour mapping

NB Presence sensor in personal office is level 3, not 0!

Intelligent Campus

Going beyond Data Protection

Challenges for traditional DP approach

- Can't guarantee people see notices
- Collection often unavoidable => Consent invalid
- Retrospective rights (e.g. SAR & objection) may be limited in practice & benefit
  - Privacy-respecting implementations actually make these harder!

Can we offer prior control as well?

- Occupants of space should be able to decide/challenge how & why it is monitored
- Achieve consensus on purposes, implementation, review and benefits

Cormack AN (?2019) "Ethics and the Intelligent Campus" in review …

Well-being

And other purposes of analytics

Very wide range

» From "take a break" apps to suicide risk flags

Messaging/communication may be the biggest challenge

» High risk of creating the stress (or worse) that you're trying to avoid

High value + high risk

» Likely candidate for DPIAs and prior approval by ICO

Data Protection probably not the biggest issue

» If student/staff health service isn't ready for this, don't do it!

References

Blog

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

Papers

» Incident response https://script-ed.org/article/incident-response-protecting-individual-rights-under-the-general-data-protection-regulation/

» Learning analytics http://www.learning-analytics.info/journals/index.php/JLA/article/view/4554

» Big data https://jirpp.ubiquitypress.com/articles/abstract/10.21039/irpandp.v1i1.9/

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

Except where otherwise noted, this work is licensed under CC-BY-NC-ND