Thinking with GDPR

Andrew Cormack, Chief Regulatory Adviser, Jisc

“This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of such data.”

“This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of such data.”

“This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of such data.”

It’s about … Controllers, not subjects

- Accountability: show we are thinking
  - About design, safeguards, operation and review
  - About impact on individuals and groups
  - Data Protection Impact Assessment (DPIA)
- Purpose Limitation: why are we doing this?
  - Clear statement/understanding of purpose(s)
  - Stick to those
- Lawful basis: why are we allowed to do it?
  - Each has its own requirements & guidance

Contract delivery
Legal Obligation
Protect life (“vital interests”)
Public Interest
Legitimate Interest

GDPR Art 6(1)

… Allowing Necessary Processing, not preventing it

Necessary means…

- "No less intrusive way to achieve purpose"
  - Least data
  - Least processing
  - Least disclosure
  - Least storage
- Lots of technologies to help…

Attributes: what, not who
Pseudonyms: recognise, not identify
Statistics: count/average/etc.
Roles: e.g. for policy enforcement
Federations: see later…
etc.

Jisc

… Notice, not (mostly) choice

“Natural consequences”…

- Always inform people…
  - Who (you are)
  - What (you are doing, inc.legal basis)
  - Why (purpose(s))
  - How long (it will last)
  - Who else/Where (is involved)
  - How (to exercise their rights)
- Occasionally seek Consent…
  - When they actually **have** a choice
  - Typically, if offering a **deeper** relationship
  - **Not**, to find out if any relationship is OK
    - If you (still) need to ask that, it probably isn’t

> “Customers expected us to do the right thing on their behalf, not just give them the info to choose for themselves (arguably an abdication of corporate responsibility).”
>
> Guy Singh-Watson, 2020

Jisc

… Doing what Users and Customers Expect

Less data collection/flow/disclosure

More effective use of information

More confidence and trust

Jisc

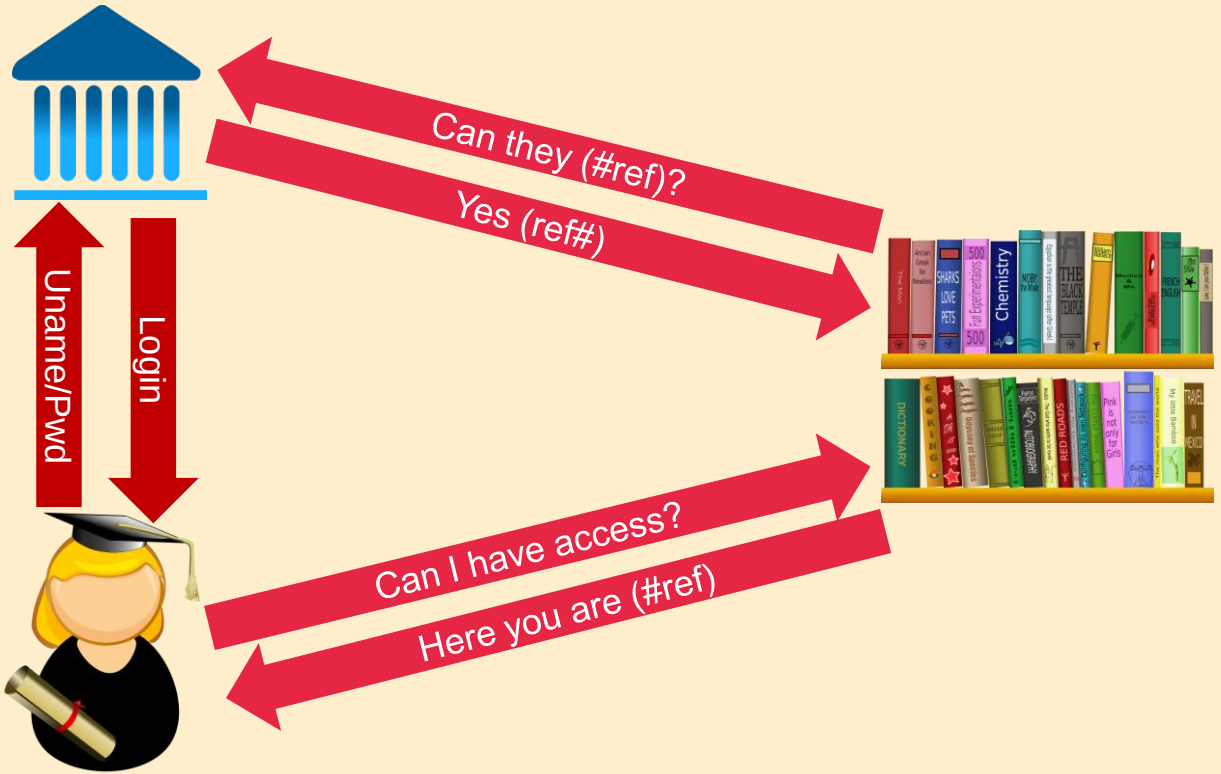
Examples

Improving on Traditional Authentication/Authorisation

Lots of (mostly unnecessary) information disclosure

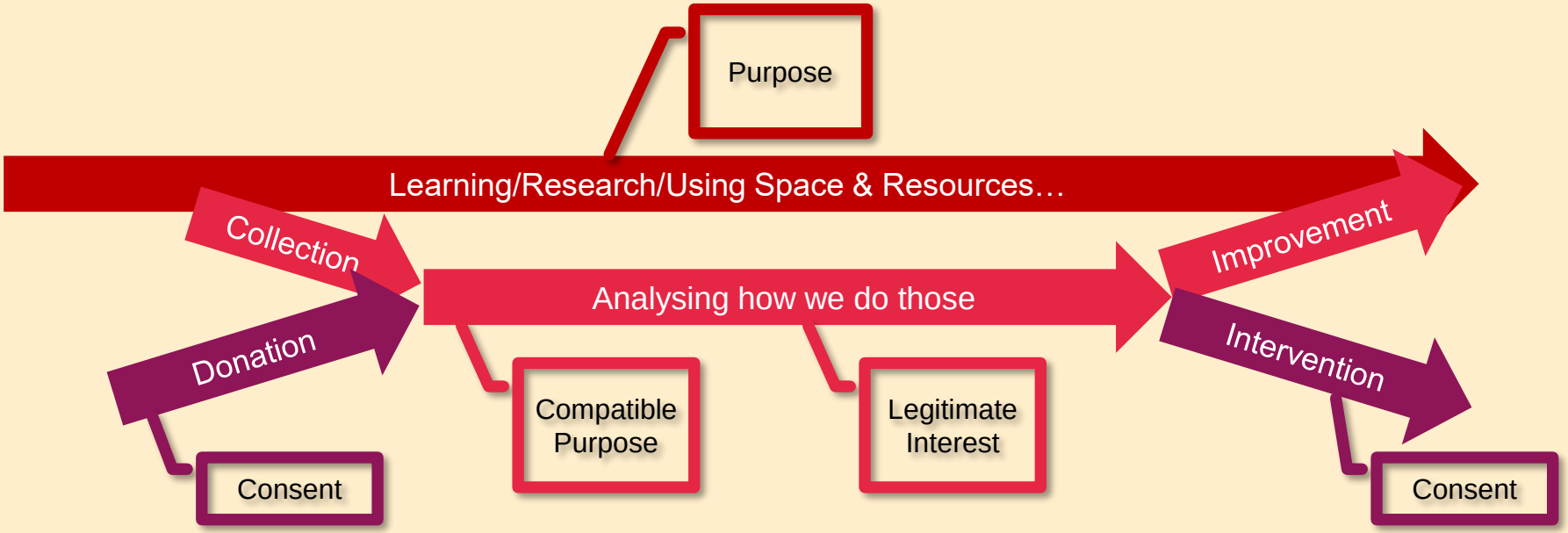
Federated Authentication/Authorisation

Working together to get the (necessary, trusted) information we need…



Safe, Confidence-building Analytics

Looking at how we do things, to make them better…



References

- Legal basis: https://regulatorydevelopments.jiscinvolve.org/wp/2019/10/23/gdpr-whats-your-justification/

Federations

- https://regulatorydevelopments.jiscinvolve.org/wp/2018/03/23/federated-authentication-and-the-gdpr-principles/

Analytics

- Paper: https://learning-analytics.info/index.php/JLA/article/view/4554
- CoP: https://www.jisc.ac.uk/guides/code-of-practice-for-learning-analytics
- DPIA: https://repository.jisc.ac.uk/7150/1/data_protection_impact_assessment_learning_analytics.pdf

Blog

- https://regulatorydevelopments.jiscinvolve.org/wp/tag/data-protection-regulation/

Andrew Cormack

Chief Regulatory Adviser

@Janet_LegReg

Lumen House, Library Avenue, Didcot

OX11 0SG UK

Andrew.Cormack@jisc.ac.uk

jisc.ac.uk