

05/09/2017

Implementing the GDPR

Andrew Cormack, Chief Regulatory Adviser, Jisc Technologies, @Janet_LegReg

New law, in force 25/5/18

Not
complete

- ~50 areas for UK to decide on (DPBill this autumn)
- Regulator (ICO) guidance not expected till Dec/Jan

Wider definition of personal data

- IP/MAC/eMail addresses likely to be covered

Organisations accountable for all their processing

- Look at information lifecycles, not just asset registers

Much stricter requirements for consent

- Look at other justifications for processing

Information Lifecycles



Collect

Process

Dispose



Collect

Process

Dispose

- » Why are we doing this?
- » What data do we need?
- » Who do we get it from?
 - › Direct?/Indirect?

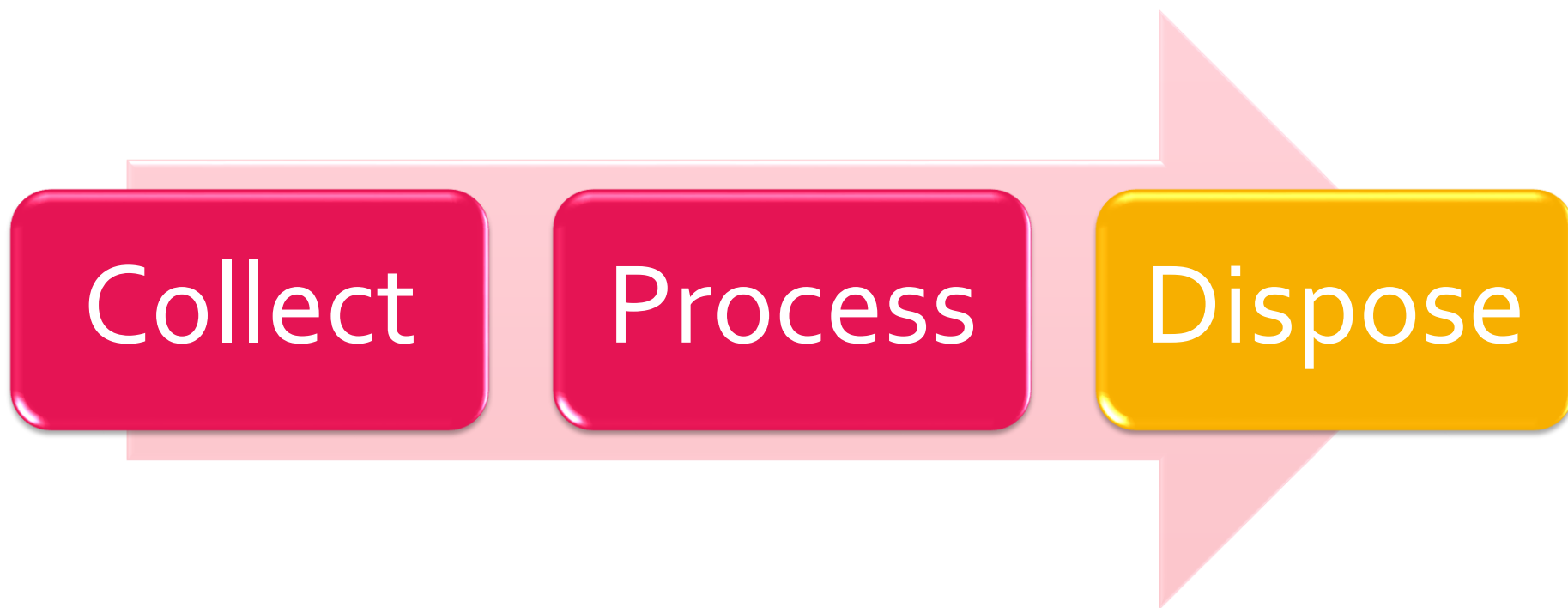


Collect

Process

Dispose

- » Why are we doing this?
- » How are we processing?
 - › Where are we processing?
 - › How do we keep it secure?



- » When are data no longer needed?
- » How do we dispose of them?
 - › Delete?
 - › Aggregate?
 - › Anonymise? Need to keep reviewing re-identification risk

Collect

- Why?
- What?
- Who?

Process

- Why?
- How?

Dispose

- When?
- How?



Share

- » Continuing responsibility
 - › E.g. secondary uses, partner organisations
- » Internal sharing
 - › Start another Lifecycle
- » External sharing
 - › Transfer responsibilities through agreement/contract



Disclose

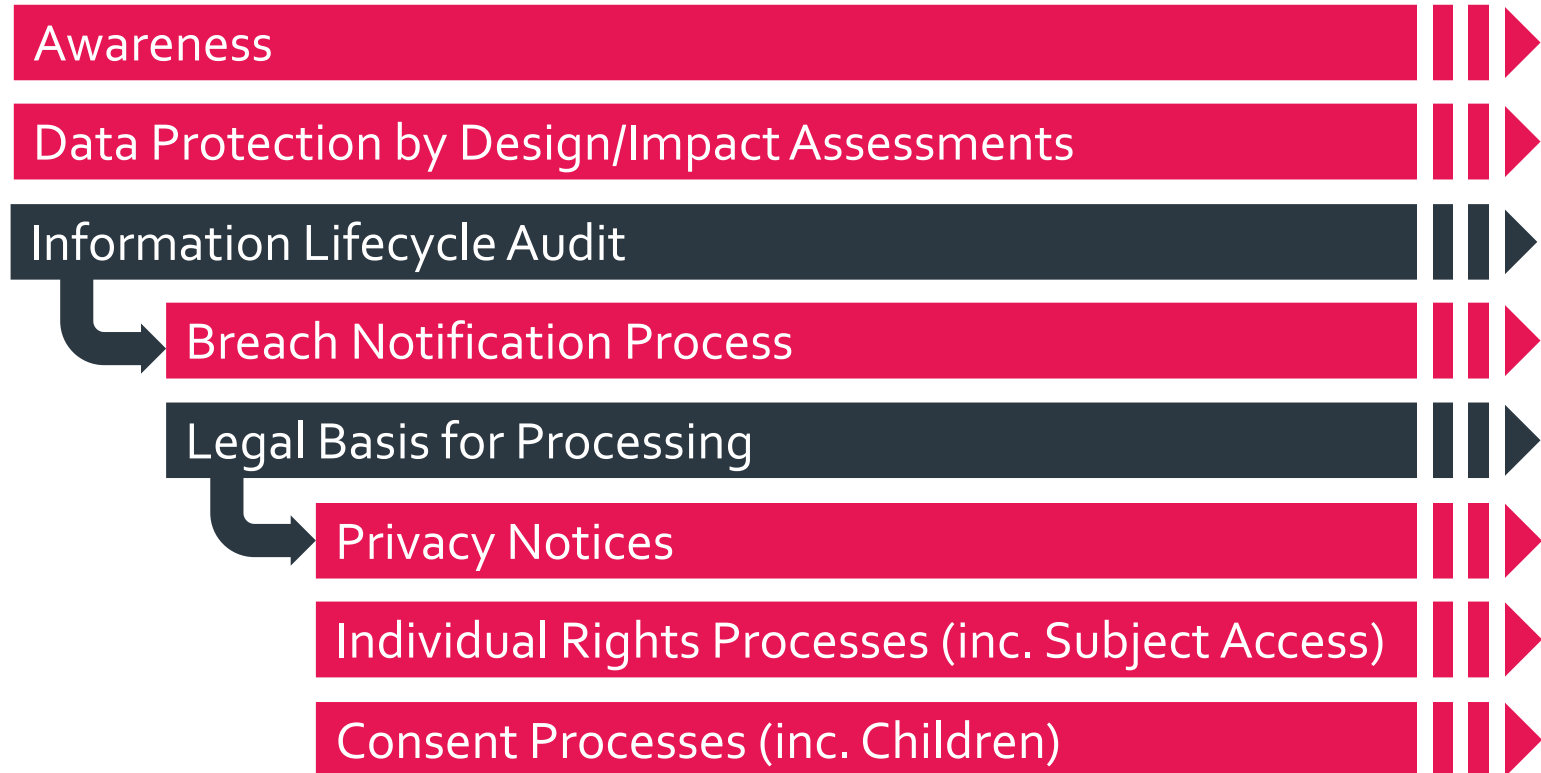
- » Responsibility ends after disclosure
 - › E.g. law enforcement
- » Need a legal exemption

Justifications for Processing

- » Six bases for processing
 - › *Necessary* for: **contract, law**, life, public interest, **legitimate interest**
 - › **Consent** (may imply *not* “necessary”?)
 - › Different duties, rights, notice requirements for each

- » Complex activities/services may well use more than one, e.g.
 - › Can't provide service without it (contract)
 - › Can't secure service without it (legitimate interest)
 - › Can make service prettier with it (consent)

Next Steps



Regulators have promised guidance on

- Transparency: Privacy Notices
- Data subject rights
- Consent/children

At least prepare for when these arrive (Dec/Jan)

Maybe implement based on drafts/old guidance

- » GDPR text: <https://ji.sc/gdpr-text>
- » Jisc “A year to get your act together”:
<https://www.jisc.ac.uk/blog/a-year-to-get-your-act-together-how-universities-and-colleges-should-be-preparing-for-new-data-regulations>
- » Jisc GDPR implementation plan:
<https://community.jisc.ac.uk/blogs/regulatory-developments/article/gdpr-12-steps-illustrated>
- » Jisc GDPR specific topics:
<https://community.jisc.ac.uk/blogs/regulatory-developments/tags/GDPRtopics>
- » ICO on GDPR: <https://ico.org.uk/for-organisations/data-protection-reform/>
- » Article 29 WP: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Andrew Cormack
Chief Regulator Adviser, Jisc Technologies

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

Andrew.Cormack@jisc.ac.uk

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

info@jisc.ac.uk jisc.ac.uk



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