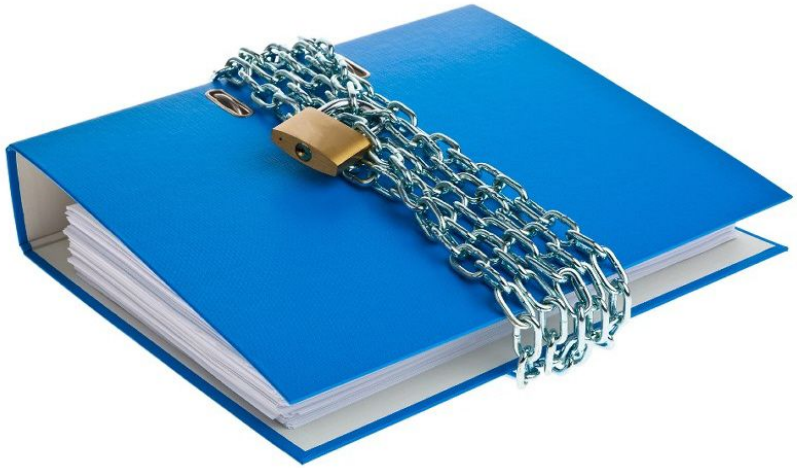
OXFORD BROOKES UNIVERSITY

General Data Protection Regulation Briefing

NEON Disability Working Group - 23 Feb 2018

GDPR Overview I



- The most significant change to data protection law since the introduction of the 1998 Data Protection Act
- Its aim is to strengthen current data protection legislation, improve privacy rights and better safeguard personal data

Overview II

- The new legislation will allow the ICO to issue fines of up to 4% of organisational turnover (c. £8m for Oxford Brookes)

- It becomes effective on the 25th May 2018

Key Changes

Data Governance	• Appointment of Data Protection Officer • Training & awareness • Data processing register and audit
Lawful Processing	• Identify legal basis for processing personal data (staff, students, third parties) • Evidence consent where relied upon
Privacy Notices	• Identify where privacy notices are necessary (staff, students and third parties) • Make available (paper and electronic)
Contracting & Procurement	• Review existing contracts and ascertain current compliance • Conduct privacy impact assessments

The 7 GDPR Principles

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity & confidentiality
- Accountability

Lawfulness, Fairness & Transparency

- Permitted legal basis
- Reasonable expectations
- Privacy notices

Sensitive Personal data

- Racial or ethnic origin
- Religious beliefs
- Trade union membership
- Genetic or biometric
- **Health (inc. disability)**
- Offending
- Sexual life

Processing Sensitive Personal data

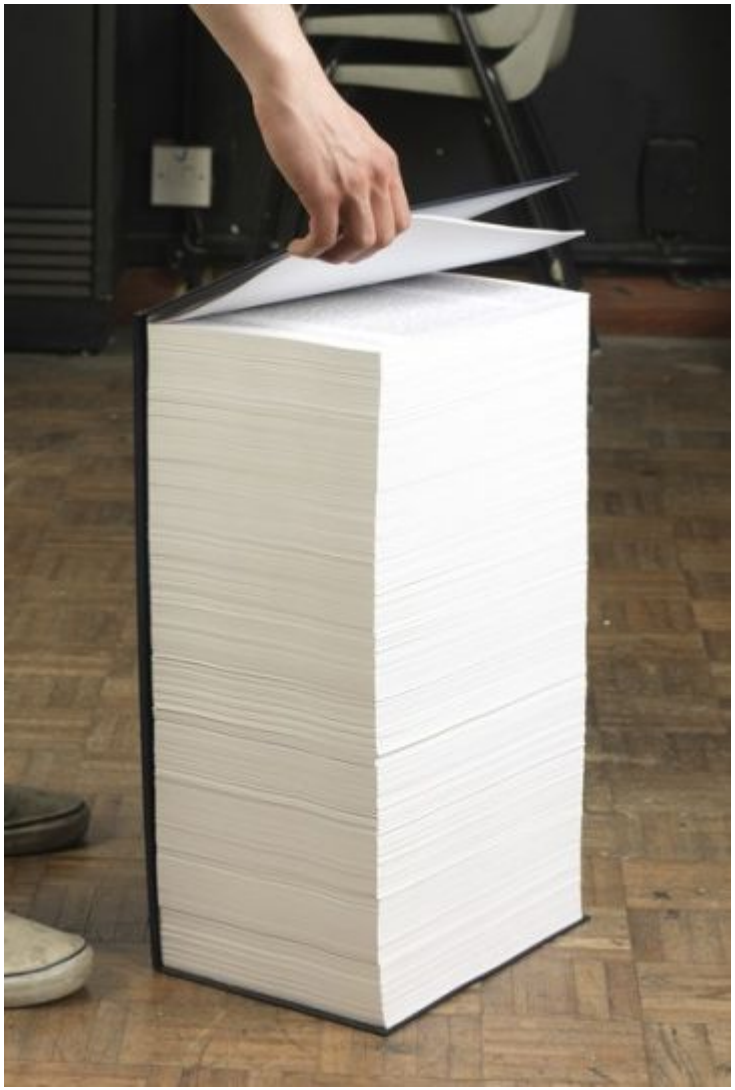
- Explicit consent
- Right or obligation relating to employment
- Necessary for medical purposes; where undertaken by a person who is:
  (a) a health professional, or
  (b) a person who in the circumstances owes a duty of confidentiality

Purpose Limitation

- Personal data must be collected for a specified purpose
- No further processing for *incompatible* reasons

Data Minimisation

Only data necessary for the specified purpose must be collected and stored



Accuracy

- Personal data must be accurate and up to date
- Data subjects have the right to update personal data where appropriate

Storage limitation

- Data should only be stored as long as *necessary*
- After this time it should be deleted or anonymised

Integrity & Confidentiality

Use *appropriate* technical and organisational security controls

- Policies & procedures
- Access control
- Encryption
- Backup and recovery
- Supply chain security

Accountability

- Evidencing consent
- Keeping processing register up to date
- Third party due diligence

Third Party Processing - A quick Primer

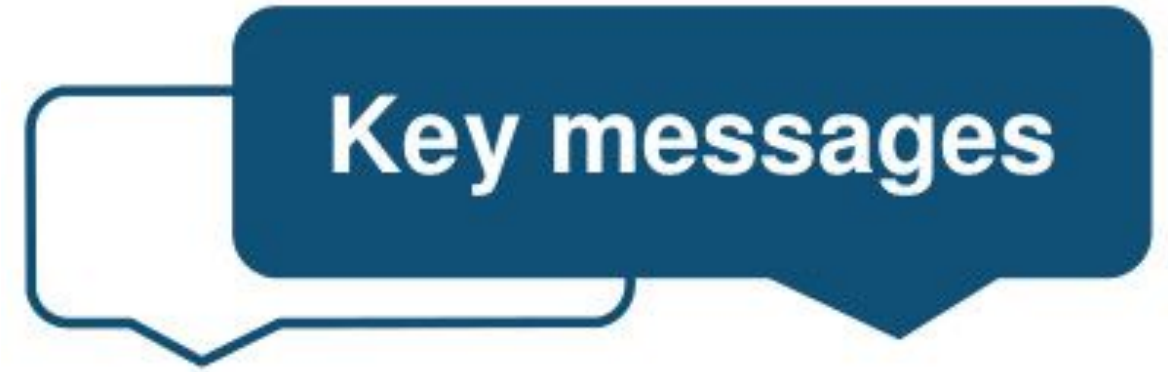
Who do we share personal data with?

- Consultants
- Offsite/cloud hosting
- Apps and extensions
- Survey providers
- Other HEIs
- ???

Third Party Processing - Due Diligence

How do we know they will safeguard our personal data?

- Contract (article 28)
- Independent security certification
- InfoSec assurance



- By and large GDPR is just existing best practice in data protection
- Data subjects must be kept informed of why their personal data is needed, who will have access to it and how to exercise their rights
- Compliance is everyone’s responsibility

Questions?