GDPR – Changes, Impact & Progress

Tim Rodgers Compliance and Information Governance Manager
What I’ll cover today

• Introduction to the regulation (and the DP Bill…)
• Key changes
• Implications on institutional librarians
• How Imperial are embracing these changes
• Q&A
Our people

Students
15,734 full-time (2015-16)
  • 9,320 – undergraduate
  • 3,240 – taught postgraduate
  • 3,174 – research postgraduate
  • Students from 136+countries

Staff
  • 3,777 academic and research staff
  • 3,770 support staff

Alumni
Over 190,000 alumni
A major shift in Data Protection law

- Years of formulation
- 88 pages
- Uniform approach to handling EU citizen data for member states and beyond
- Derogations for nation state variance (e.g. age of child)
- DP Bill fills in the gaps (e.g. law enforcement and criminal records data), and makes ‘local’ arrangements – currently going through Parliament… will it be ready by May 25th?
Privacy and Innovation

- Obvious main thrust of GDPR – *to bolster privacy rights*
- BUT ALSO…
- Harmonising legislation
- Exemptions for scientific, historical and health research

Aim to create a Digital Single Market…
GDPR…what’s new?

• A single set of rules governing all EU nations, and all organisations that process personal data of EU citizens
• Definitions of data
• Sanctions
• Data protection safeguards
• Privacy by Design
• Consent
• Clarity of rights for data subjects
• Incident reporting
Definitions of data

Personal data includes online identifiers and location data (IP addresses, mobile device IDs, cookie IDs)

Pseudonymous data – personal data subject to technological measures so it no longer directly identifies an individual without the use of additional information.

Genetic and biometric data – treated as special categories of personal data
Sanctions

- Isn’t (and has never been) just about loss of data
- For controllers and processors
- Two bands of fine – 2%/€10m or 4%/€20m which ever is greater

4% can apply to processing without consent, violating principles of privacy by design, unlawful cross-border data transfers, violation of data subject rights

2% can apply for not having records of processing in order, not notifying ICO or data subject of a breach, or not conducting an impact assessment
Data protection safeguards

“To implement appropriate technical and organisational measures”

These safeguards should be appropriate to the degree of risk associated and might include:
- pseudonymisation and/or encryption of personal data
- ensuring ongoing CIA and resilience
- restoring availability of and access to data in a timely manner following incident
- introduce regular testing and evaluation of these systems
Privacy by Design

- Essential an organisation ‘shows its working’
- DP concerns should be weaved into the design of all procedures, projects, systems
- Good DP compliance by default
- PIAs required for new activities and undertakings
- Especially for new activities and undertakings

- Does this, or should this stand part of ethics work for research?
Consent

• Where required it must be:

Any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.

Organisations need to be able to show how and when consent was obtained. Not necessarily explicit, but relating to data obtained for specific, explicit and legitimate purposes.

Individuals must be able to withdraw consent and have a right to be forgotten (subject to qualification).
Rights for data subjects

- To be informed – for privacy notices to be more robust and transparent
- To have explained purposes & conditions of processing, intended retention, right
- To erasure
- To data portability
- To restriction
- To rectification
- To access
- To object
- To prevent automated processing
Breach reporting

- Mandatory unless there is no risk to the rights of data subjects
- Articles 33 & 34 indicate pseudonymised data is exempt from this (unless other information would enable someone to identify individuals)
- Notify ICO within 72 hours (and possibly NHS Digital?) – ensure procedures set up internally, and with your suppliers
1. Awareness
You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2. Information you hold
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3. Communicating privacy information
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4. Individuals' rights
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5. Subject access requests
You should update your procedures and plan how you will handle requests within the new timescale and provide any additional information.

6. Legal basis for processing personal data
You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

7. Consent
You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

8. Children
You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

9. Data breaches
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10. Data Protection by Design and Data Protection Impact Assessments
You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11. Data Protection Officers
You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation’s structure and governance arrangements.

12. International
If your organisation operates Internationally, you should determine which data protection supervisory authority you come under.
GDPR for Librarians

- Right to be forgotten vs digitising assets – the ECJ ruled in the Google Spain case that individuals had a right to be forgotten when websites made outdated information available (unless public interest in keeping information disclosable)
- Significant provisions regarding research – supports research subject to appropriate handling and risk management
Key articles and recitals

• Recital 159 – broad definition of research
• Article 6(4), Recital 50 – organisations processing personal data for research purposes may avoid restrictions on secondary processing and on processing sensitive categories of data.
• Article 89 – as long as there are safeguards, organisations may override a data subjects right to object to processing and seek erasure of personal data
• Article 6(1)(f), Recitals 47, 157. Organisations to process personal data for research purposes without the consent of a data subject
• Article 49(h), Recital 113 – for some processing personal data can be transferred to third countries for research purposes without any other transfer mechanism in place.
Archiving in the public interest (Recital 158/DP Bill)

- No specific provision (as yet) but could be regarded as a continuation of Section 33 of the Data Protection Act 1998 enshrined in the DP Bill
- Process personal (and special categories of data) without consent where necessary for archiving purposes in the public interest
- Subject to appropriate safeguards for the rights and freedoms of data subjects
- Expectation that the DP Bill will deal with proper definitions of archives and the activity of archiving
- Should mean better protection for archives, essential given potential penalties
Research as a basis for processing

- Article 6(1) outlines lawful bases for processing
- Article 6(4) allows data obtained through a lawful basis to be used for a secondary research purpose.
- Research not a lawful basis in itself, but could be regarded as a legitimate interest (Article 6(1)(f))
- What if you get consent, but are not clear at the time of collection about the research? (Recital 33). Article 6(4) talks about purposes that are compatible
- Indeed Article 89 confirms that research in the public interest, for scientific or historical research purposes would not be considered incompatible – subject to safeguards set out in the same article
GDPR-related activity at Imperial

- In March, the Personal Data Assessment Questionnaire was launched for completion across College.
- Returns are being collated into tailored gap-analysis for each Support Service or Faculty.
- Services to students were prioritised, as were privacy notices to ensure compliance with the regulation for the current academic year.
- Consideration given to legal basis for processing data, to ensure we have both clarity and transparency for data subjects.
- Data breach process updated, including guidance, a new reporting form and plan.
- Data Protection Officer role started February.
Definition of an information asset (& register)

- An information asset is defined as a logical collection of information recorded on written / printed documents or in electronic files / databases / documents.

- Information Asset Register is a list of logical information collections across the College, e.g. employee paper records in H/R, filed supplier invoices in Finance, data held for research in an academic department, etc. Information Asset register contains information description, ownership, accessibility, whether it contain sensitive data or not, how it is kept secure and its retention
Definition of IAO (from IG Policy Framework)

- IAOs are senior/responsible individuals working in a relevant business area. Their role is to understand what information is held within their business area, what is added and what is removed, how information is moved, who has access and why. As a result they are able to understand and address risks to the information that information is used within the law for the public good, and provide written input to the SIRO annually on the security and use of their assets.

- An IAO will be responsible for an information asset in terms of:
  - Identifying risks associated with the information asset
  - Managing and operating the asset in compliance with policies and standards and;
  - Ensuring controls implemented manage all risks appropriately.
Definition of IAA (from IG Policy Framework)

- IAAs work on a day-to-day basis with information contained in an information asset. They have day-to-day responsibility for the asset, and make sure that policies and procedures are applied and adhered to by staff and can recognise actual or potential security incidents. They are responsible for reporting such incidents to their IAO and consulting the IAO on incident management. The role is flexible and will undoubtedly be performed in addition to existing duties.
Our offer to IAOs

- You (are/agree to be) the IAO for this asset – a formal notification
- Management of the asset (risk, training, access etc…)
- Onward reporting to the SIRO
- To use the online system!!!

IN EXCHANGE
- Training
- Support from Legal, ICT, RM etc…
- Peer support
DPIA

• All projects/processes require a DPIA – a Data Privacy Impact Assessment
• Embedded in ICT Project Management methodology
• Looking to establish in other project management approaches (e.g. Operational Excellence)
• To think, at every stage, about how the privacy of the data subjects is impacted by the processing of the data.
• DPIA functionality in the IAR
The final few months…

- Launching the information asset register
- Training staff
- GDPR contract review with external suppliers
- Embedding IAO governance
- Refreshing policies
- Considering wider application of DPIAs to wider business processes
- Project around hardware ICT assets to improve tracking over lifecycle
Thanks for listening

Any questions?