IT Community Development Project
GDPR & UIS Initiatives

Margaret Griggs, IT Community Development Project Manager
James Knapton, Information Compliance Officer, Registry’s Office
Madeleine Taylor, Information Services Compliance Officer, UIS
Contents

• Welcome and introduction
• Project Update
• Skills profiling interest contact Rinku Raina: rr541@cam.ac.uk
General Data Protection Regulation: Changes and Implementation

James Knapton, Information Compliance Officer, Registry’s Office
• What is the GDPR?
• Key changes from the Data Protection Act 1998
• GDPR Data Protection Working Group
What is the GDPR?

- EU General Data Protection Regulation applies *in full* from 25 May 2018
- Data Protection Act 1998 repealed on same date
- Will apply in UK despite Brexit
- Enhanced and more prescriptive standard of data protection law
- Based around existing concepts of data protection principles and data subject rights
- Some different rules for ‘public authorities’ as opposed to private businesses
  - Neither GDPR nor wider EU law defines public authorities
  - Working assumption is HEIs will be public authorities for most GDPR purposes
- EU Member States can add additional rules and exemptions – currently awaited
## Key changes from DPA: Principles

<table>
<thead>
<tr>
<th>DPA</th>
<th>GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personal data shall be:</strong></td>
<td><strong>Personal data shall be:</strong></td>
</tr>
<tr>
<td>1: processed fairly and lawfully</td>
<td>1a: processed fairly, lawfully and transparently</td>
</tr>
<tr>
<td>2: processed only for specified and lawful purposes</td>
<td>1b: processed only for specified, explicit and legitimate purposes</td>
</tr>
<tr>
<td>3: adequate, relevant and not excessive</td>
<td>1c: adequate, relevant and limited</td>
</tr>
<tr>
<td>4: accurate</td>
<td>1d: accurate and rectified if inaccurate</td>
</tr>
<tr>
<td>5: not kept for longer than necessary</td>
<td>1e: not kept for longer than necessary</td>
</tr>
<tr>
<td>6: processed in accordance with data subjects’ rights</td>
<td>Not a principle but covered elsewhere in GDPR</td>
</tr>
<tr>
<td>7: processed securely</td>
<td>1f: processed securely</td>
</tr>
<tr>
<td>8: not transferred outside the EEA without adequate protection</td>
<td>Not a principle but covered elsewhere in GDPR</td>
</tr>
<tr>
<td>Not covered in DPA</td>
<td>2: data controller must be able to demonstrate compliance with 1a-1f</td>
</tr>
</tbody>
</table>
Key changes from DPA: Legal basis for processing (1)

• Under DPA, need to meet a ‘condition for processing’ for personal data use
  ➢ With consent
  ➢ To operate a contract
  ➢ To meet a legal obligation
  ➢ To protect the data subject’s vital interests
  ➢ To perform a public interest task
  ➢ To further the legitimate interests of the data controller

• Under GDPR, these are reformulated as ‘legal bases for processing’
  ➢ ‘Legitimate interests’ invalid for public authorities ‘in the performance of their tasks’
  ➢ Higher standard of consent – a genuine affirmative choice that is withdrawable
Key changes from DPA: Legal basis for processing (2)

- Special category data
  - Racial / ethnic origin, political opinions, religious / philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life / sexual orientation
  - Need to meet an additional legal basis – e.g. with explicit consent
- Member States can specify particular or add extra legal bases for data processing
- University needs to:
  - Reconsider its legal basis for each type of data use for each type of data subject (applicants, students, alumni, staff, research participants…)
  - Realign its engagement mechanisms with different types of data subject – e.g. remove inappropriate blanket consents and rely instead on contracts
Key changes from DPA: Privacy notices

- DPA: need to tell data subjects who you are, how you’ll use their data and who you’ll share it with

- GDPR: need to do this but also:
  - Notices must be transparently worded and accessible
  - Notices must be given at point of data collection from the data subject or within one month if the data are not directly collected
  - Notices must cover numerous subjects, including the legal basis relied upon, retention periods, data sharing, the existence of data subject rights…

- All University privacy notices need to be rewritten and (where possible) rationalised and standardised
Key changes from DPA: Rights

• Enhanced rights of:
  - Access
  - Rectification of inaccurate personal data
  - Restriction pending verification or correction
  - Objection (including to profiling and direct marketing)

• New rights of:
  - Erasure (‘the right to be forgotten’)
  - Portability

• All GDPR rights are qualified, and Member States can add further exemptions

• University needs to assess its systems and processes to enable the rights to be fulfilled if exercised
Key changes from DPA: Accountability

- New focus in GDPR on accountability measures
  - Policies and procedures to promote data protection by design and default
  - Detailed rules surrounding contracts with joint data controllers and with data processors
  - Maintenance of a detailed personal data register
  - Newly prescriptive requirements about security
  - Certain personal data breaches to be notified to ICO within 72 hours
  - Newly prescribed Data Protection Impact Assessments for ‘high risk’ processing
  - Newly prescribed senior role of Data Protection Officer
- All require new / revised policies, guidance, records, training, ways of working…
Key changes from DPA: Specific exemptions

• Member States can vary rules for data processing for specific activities
  ➢ Crime
  ➢ Journalism and freedom of expression
  ➢ Employment
  ➢ Research – although research is generally quite protected already

• National legislation awaited
Key changes from DPA: Penalties

• Higher fines
  – ICO fines of up to €20m for certain infringements, including those about principles, legal basis and rights
  – ICO fines of up to €10m for other infringements, including those about accountability

• New roles for pan-European organisations to regulate and harmonise compliance
GDPR Data Protection Working Group (1)

• Established summer 2016

• Chaired by the (Acting) Registrar

• Members from Registrar’s Office, LSO, Student Registry, CAO, ESP, UIS, CUDAR, Research Office, HR, UL, OIS, School Offices

• Observers from CA and CUP
GDPR Data Protection Working Group (2)

• Terms of Reference

➢ “To develop, scrutinise and approve the necessary changes to the University’s policies, procedures, guidelines and training in time for the implementation of the EU’s General Data Protection Regulation. Where formal Committee oversight is required for any particular change, to develop, scrutinise and recommend the necessary change to the relevant Committee”

• By autumn 2017

➢ Complete fundamental changes (so as to be ready for start of new applications cycle and academic year 2017-18)

• Autumn 2017 to May 2018

➢ Complete other changes

➢ Train and raise awareness
Further information

• Website (Raven required)


• Email

  data.protection@admin.cam.ac.uk
Implications of GDPR for UIS

Madeleine Taylor
Information Services Compliance Officer

June 2017
What is the University doing to get ready?

- Set up GDPR Working Group chaired by Emma Rampton
- High Level plan from GDPR-WG ‘owned’ by James Knapton
- Many key areas which may have impact on systems are still in work-in-progress
- Chris Edwards as UIS representative on GDPR-WG
- Madeleine Taylor Certified GDPR Practitioner in UIS
- Barry Skingle only non-UIS IT representative GDPR-WG
Sections of the University GDPR Working Group High Level Plan

- **Part A - Changes to policies and procedures**
  1. Interactions with applicants and students
  2. Interactions with alumni and supporters
  3. Interactions with job applicants and staff
  4. Interactions with website/system users and members of the public
  5. Procedures for data subject rights
  6. Interactions with research subjects
  7. Contracts between organisations
  8. Organisational processes

- **Part B - Changes to guidance and training**
  9. Guidance and training
  10. Communications
Part A - Changes to policies and procedures

1. Interactions with applicants and students
   - This will require a change to CamSIS.
   - There may be other system implications following implementation of new privacy notices and consent requirements

3. Interactions with job applicants and staff
   - This may require a change to CHRIS, RAS or our other HR systems. Need for changes not yet confirmed
5) Interactions with website/system users and members of the public

- UIS need to create amended *privacy notices* for websites and IT systems, publish them and ensure systems adhere to them
- UIS need to guide local IT functions in doing the same

6) Procedures for data subject rights

- UIS need to assess whether major IT systems are technically capable of fulfilling the rights of the data subject (especially of erasure, portability and restriction)
- This requires University (via the GDPR-WG) to assess how it wishes to fulfil those rights

7) Contracts between organisations

- UIS need to amend template data processing agreements/clauses with contractors /suppliers, through collaboration with LSO, Procurement and UIS Departmental Ops
9) Organisational processes

- UIS to create new **personal data register** encompassing personal data held both in **core IT systems** and **across all** academic/administrative activities.

- UIS to support creation of amended and standardised **personal data breach procedure** to enable ICO notification within 72 hours and prompt notification to affected users where necessary.

- UIS to **assess** IT systems against GDPR security and privacy requirements, including embedding “Data Protection by Design” into new or enhanced systems. And UIS to **assist local IT functions** to do the same.

- UIS to support creation of updated **information security policy/policies**, that are aligned to GDPR, and to create associated IT security sub-policies.

- Revised university **records retention** policy may require system changes.
UIS Implications, Part B

• Part B - Changes to guidance and training

9. Guidance and training

• UIS to create and launch amended guidance and training on information security, including breach notifications (to be consistent with amended complementary guidance and training on data protection from James Knapton)

10. Communications

9. UIS need to support JK’s awareness-raising communications plan and ensure its messages are consistent with those of the CyberSecurity Programme
In Conclusion – Key Themes from GDPR for UIS

1. Information Asset Register
2. Personal Data Breach Response Procedure
3. GDPR Checklist for systems
4. Building Data Protection By Design into our project and solutions
5. Privacy Notices
6. Review of UIS Contracts for GDPR compliance
7. Revisions to our Online Information Security Training
8. Update Information Security Policies
What Has Been Done In UIS & What Is Yet To Do?
Information Assets

**ACTION**
- Interviews with DAs and COs across University
- Visibility raised at interviews about Admin Information Assets, the IAR and GDPR

**RESULT**
- Initial view of Information Assets and issues in rolling out IAR
**Information Asset Register (IAR)**

**ACTION**
- Information Asset Project is:
  - Information Asset Register
  - Information Asset Ownership
  - System Security Checklist (SSC)

**RESULT**
- **Tender process** for IAR
- Piloting IA Ownership Role

**FURTHER ACTION**
- Tested SSC against top UIS business systems and creating guidance documents
Personal Data Breach Response Procedure

ACTION

• Incident Process Published and SOC initiated

RESULT

• Little or no alteration needed to conform with Breach Notification
GDPR Checklist

**ACTION**
- Initial draft being worked into simple, easy-to-use on-line form
- **Testing** on a few UIS systems as a pilot very soon

**RESULT**
- Expected to be used by IT community on existing systems to help them check GDPR compliance

**PLAN**
- UIS to apply to further UIS systems
Data Protection by Design (DPbyD)

**ACTION**
- DPbyD into Project Board Process
- Engagement with Procurement

**RESULT**
- Project Board and Processes already including DPbyD

**PLAN**
- Await DPO on final version of Data Protection Impact Assessments (DPIAs) for use within DPbyD
Privacy Notices, Contracts, Training and Policies

**ACTION**
- **UIS contracts** have been listed
- Information Security Training has been launched

**PLAN WG**
- GDPR working group to oversee creation of model **privacy notice** and **template** for websites and systems

**PLAN UIS**
- **UIS contracts** to be re-worked
- Information Security Training to reference Data Protection Training and Breach Notification
- Re-work UIS **Privacy Notices**
- Update Information Security Policies
IT Community Development Seminar Feedback

• Feedback Questionnaires to complete

• Email link will be sent to attendants
  http://cambridge.eu.qualtrics.com/jfe/form/SV_3pXpK36C7K CZLKZ

• Or you can scan the QR code