UNIVERSITY OF CAMBRIDGE

Data Protection Annual Compliance Checklist 2023-24

Briefing sessions, 10 and 14 May 2024

James Knapton, Head of Data Protection and Information Compliance, Governance and Compliance Division

Session outline

- Overview of data protection law
  - The legislation
  - Principles
  - Rights
  - Accountability obligations
- The Checklist
  - Versions
  - Purpose and structure
  - Actions
  - Timescales and next steps

The legislation

- Since 1 January 2021
  - UK GDPR *plus*
  - Data Protection Act 2018
- Standards for handling ('processing') of information ('personal data') about living identifiable individuals ('data subjects') by organisations ('data controllers')
  - Data protection principles
  - Data subject rights
  - Accountability obligations
- Certain types of activity exempt from certain aspects of the law
- Regulated by the Information Commissioner's Office as well as the courts

Principles

- Personal data shall be
  - Processed fairly, lawfully and transparently – need an underpinning legal basis plus an extra basis for sensitive ('special category') personal data
  - Processed only for specified, explicit and legitimate purposes
  - Adequate, relevant and limited ('data minimisation')
  - Accurate
  - Not kept for longer than necessary
  - Processed securely – confidentiality, integrity and availability
- Data controller must be able to *demonstrate* compliance with principles

Rights

- Data subject rights
  - Being informed about how personal data are being used – privacy notices
  - Access
  - Rectification of inaccurate personal data
  - Erasure (‘the right to be forgotten’)
  - Restriction pending verification or correction
  - Portability
  - Objection (including to profiling and direct marketing)
- Rights are qualified

Accountability

- Accountability measures
  - Data protection by design and by default
  - Data Protection Impact Assessments for ‘high risk’ personal data processing
  - Prescribed contents of contracts with ‘data processors’
  - Rules about personal data transfers outside the UK
  - Maintenance of a personal data register
  - Reporting certain personal data breaches to ICO within 72 hours
  - Role of independent Data Protection Officer

Checklist: past versions

- Version 1 launched November 2020 as recommended guidance for 2020-21
  - Consultation exercise
- Version 2 launched November 2021 as mandatory for 2021-22
  - Follow-up meetings with selected departments
  - Analysis of responses and DPO report
  - Audit Committee report and scrutiny
- Version 3 launched March 2023 as mandatory for 2022-23
  - Ratings and feedback to departments
  - Analysis of responses and DPO report
  - Deloitte internal audit exercise

Checklist: current version, purpose and structure

- Current version 4 launched April 2024 as mandatory for 2023-24
- Purpose
  - Guide annual ‘housekeeping’ actions to be carried out by individual departments to help with legal compliance
  - Keep training and awareness up-to-date
  - Meet regulatory expectations (the ICO, auditors, etc.)
- Structure
  - Specific practical actions hyperlinked to detailed guidance, templates, example texts, etc.

Checklist: actions

- 13 actions (same as last year)
  - Not all actions will be applicable to all departments
  - Some are very quick (e.g. circulating an email)
  - Some are more involved (e.g. reviewing and destroying old records)
  - Should not be starting from scratch
  - Usually led by Departmental Administrator (or equivalent), but inform Head of Department and engage colleagues as necessary
  - Recommendations within Checklist about what documentation to retain as 'evidence' of completion

Checklist: timescales and next steps

- Timescales
  - Completed Checklist (signed by DA) returned to data.protection@admin.cam.ac.uk by **Friday 26 July 2024**
  - Checkbox plus short commentary on what was done to address each action
  - It's OK for certain actions to be ongoing at that stage
- Next steps (summer-autumn 2024)
  - Review of returns by Information Compliance Office and DPO
  - Spot checks of some departments
  - Ratings/feedback provided to departments
  - Report to Audit Committee
  - Seek feedback and consider future of Checklist for 2024-25

Further information

- The Checklist

  https://www.information-compliance.admin.cam.ac.uk/data-protection/guidance/compliance-checklist

- Main data protection website (policies, guidance, tools, training)

  https://www.information-compliance.admin.cam.ac.uk/data-protection

- Email

  data.protection@admin.cam.ac.uk