UNIVERSITY OF
CAMBRIDGE

Data Protection Annual Compliance Checklist 2022-23

Briefing sessions, 5 and 13 April 2023

James Knapton, Head of Data 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: versions

- Version 1 launched November 2020 as recommended guidance for 2020-21
  - ➢ Consultation exercise summer 2021
- Version 2 launched November 2021 as mandatory for 2021-22
  - ➢ Analysis of responses and follow-up meetings with selected departments summer 2022
  - ➢ DPO report autumn 2022
  - ➢ Audit Committee report and scrutiny January 2023
- Version 3 launched March 2023 as mandatory (again) for 2022-23

Checklist: purpose and structure

- 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 – especially this year
  - Usually led by Departmental Administrator (or equivalent), but inform Head of Department and engage colleagues as necessary

Checklist: timescales and next steps

- Timescales
  - ➢ Completed Checklist (signed by DA) returned to data.protection@admin.cam.ac.uk by **Friday 14 July 2023**
  - ➢ It’s OK for some actions to be ongoing at that stage
  - ➢ Short commentary on what was done to address each action
- Next steps
  - ➢ Review of returns by Information Compliance Office and DPO
  - ➢ Assurance rating/feedback provided to departments late summer 2023
  - ➢ Report to Audit Committee autumn 2023
  - ➢ Consider future of Checklist for 2023-24

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