Data Protection Annual Compliance Checklist 2024-25

Briefing sessions, 7 and 13 May 2025

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

  - Purpose and structure

  - Past versions

  - Current version – contents and practicalities

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

UNIVERSITY OF CAMBRIDGE

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

UNIVERSITY OF
CAMBRIDGE

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.

UNIVERSITY OF
CAMBRIDGE

Checklist: past versions (1)

- 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

Checklist: past versions (2)

- 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

- Version 4 launched April 2024 as mandatory for 2023-24

  ➢ Ratings and feedback to departments

  ➢ Spot check meetings

  ➢ Chasing of incomplete actions

  ➢ Survey of respondents

  ➢ Analysis of responses and DPO report

UNIVERSITY OF CAMBRIDGE

Checklist: current version – contents

- Current version 5 launched April 2025 as mandatory for 2024-25

- 13 topics (same as last year)

  ➢ Not all actions are applicable to all departments

  ➢ Some actions are very simple, others are more involved

  ➢ Should not be starting from scratch

  ➢ Work usually led by Departmental Administrator (or equivalent), but inform Head of Department and engage colleagues as necessary

UNIVERSITY OF CAMBRIDGE

Checklist: current version – practicalities

- Exercise simplified this year

  - ➢ **Response via MS Forms by Friday 11 July 2025**

  - ➢ **Response limited to first 3 topics, plus comments on implementation of last year's feedback**

  - ➢ Feedback shortly after submission (no ratings)

  - ➢ Short spot check meetings with some departments

  - ➢ Reporting to Audit Committee

  - ➢ Consider future of Checklist for 2025-26

UNIVERSITY OF CAMBRIDGE

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

UNIVERSITY OF
CAMBRIDGE