

# U4 Seminar Preparation: Ethical Analysis

## Ricardo–Beth Records Case (GDPR & Professional Codes)

David Abiodun — 08 November 2025

### Case Study: Privacy

Ricardo works for the records department of his local government, with access to property tax records. For a scientific study, a researcher, Beth, has been granted access to numerical data but not names. She requests Ricardo to release names and addresses to contact participants, raising ethical and legal considerations.

#### 1. If Ricardo is not responsible for determining allowable access, should he release the names and addresses?

No. Disclosing personally identifiable information (PII) without lawful authority breaches UK GDPR and the Data Protection Act 2018. It also violates ACM (2018) and BCS (2023) codes requiring confidentiality and integrity. Ricardo should escalate to the Data Protection Officer (DPO).

#### 2. If Ricardo were responsible for determining allowable access, what ethical issues would be involved?

He must balance research value against privacy rights. Ethical access requires a Data Sharing Agreement, DPIA, ethics approval, and role specification. Lawful processing under Article 6(1)(e) applies only with purpose compatibility and Article 89 safeguards.

#### 3. Should Beth be allowed to contact individuals?

No. The Records Department should act as gatekeeper, contacting individuals on Beth's behalf. Direct release would exceed data minimisation and undermine confidentiality.

#### 4. What ethical issues should the Records Department consider?

Lawfulness, fairness, transparency, purpose limitation, and security per Articles 5 and 24 UK GDPR. It must ensure audit trails, staff training, and retention control.

#### 5. If one-third consent, one-third refuse, and one-third do not respond, what options are available to Beth?

Non-response cannot be treated as consent. Beth can proceed with consenting data, request reminders, amend design with ethics approval, or use anonymised datasets.

### ■■ Consequences of Ethical Breach

- **Legal consequences:** Unauthorised disclosure may result in fines up to £17.5 million or 4% of turnover under UK GDPR Article 83 (ICO, 2024).
- **Professional consequences:** Violations of ACM (2018) or BCS (2023) codes can lead to disciplinary sanctions or loss of membership.
- **Reputational consequences:** Breaches erode public trust, attract media scrutiny, and harm institutional credibility.
- **Ethical implications:** Breaching confidentiality contravenes the Belmont Report (2018) principle of respect for persons and undermines research ethics.

## References

- Association for Computing Machinery (2018) ACM Code of Ethics and Professional Conduct.
- BCS, The Chartered Institute for IT (2023) Code of Conduct.
- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.
- Information Commissioner's Office (ICO) (2024) Research Provisions and Data Sharing: Article 89 Safeguards and Enforcement Guidance.
- The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (2018) The Belmont Report.