



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCA7028

Data Security and Compliance

Week 3 : Compliance: Law and Ethics

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Learning Objective(s) and Key Concepts

Learning Objective(s)

- Explain why we need laws
- Explore the importance of the ethics

Key Concepts

- Differentiate between law and ethics
- Describe the ethical foundations and approaches that underlie modern codes of ethics
- Discuss relevant professional security organisations and their role and relationship to organisational InfoSec
- Describe why ethical codes of conduct are important to InfoSec professionals and their organisations
- Identify significant national and international laws that relate to the practice of InfoSec
- Explain the challenges and methods associated with the management of digital forensics in an organisation

The Role of Computers in Crime

- Equipment theft. Computer or network hardware is stolen.
- Equipment vandalism. Computer or other hardware is damaged or defaced.
- Data theft. Data stored on a computer is stolen.
- Data vandalism. Data (which can include software) stored on a computer is changed, damaged, or destroyed.
- Trespass. A party logically enters a computer or other system without authorisation.

Legal Compliance Landscape

Why Compliance Matters

- Legal risk: Fines, lawsuits, reputational hit.
- Example: £44M GDPR fine on Meta, 2023.

UK Data Protection Act 2018

- Data Protection Act 2018 (DPA 2018): Core UK law for data protection, implementing GDPR and governing personal data use.
- Key Features:
 - Updates and replaces the Data Protection Act 1998.
 - Strengthens individual rights (e.g., access, erasure) and organisational duties.
- Penalties:
 - Fines up to £17.5 million or 4% of annual global turnover (whichever is higher).
 - Based on severity, e.g.:
 - Breaches for commercial gain.
 - Failure to protect personal data.
 - Non-compliance with lawful processing.

General Data Protection Regulation (GDPR)

- The GDPR is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA.
- **Key Features:**
 - Applies to all organisations processing personal data of EU residents, regardless of their location.
 - Enhances data subject rights (e.g., right to access, rectification, erasure).
 - Requires organisations to obtain explicit consent for data processing.
 - Mandates data protection by design and by default.

GDPR Penalties and Compliance

- Fines up to €20 million or 4% of annual global turnover.
- Tiered penalties based on severity:
 - Up to €10 million or 2% of global turnover for less severe breaches (e.g., admin errors, lack of DPO).
 - Up to €20 million or 4% of global turnover for severe breaches (e.g., ignoring data subject rights)
- Compliance Requirements:
 - Conduct regular data protection impact assessments (DPIAs).
 - Implement strong data protection policies.
 - Appoint a Data Protection Officer (DPO) for large-scale data processing (Accountability).
 - Report data breaches within 72 hours.
- Example of GDPR compliance breach
 - British Airways £20M fine—poor security controls

GDPR Penalties and Compliance

- Accountability: Data Protection Officers, audits.
- Case: British Airways £20M fine—poor security controls.

Beyond GDPR

- UK Investigatory Powers Act 2016—surveillance vs. privacy.
- US CLOUD Act—cross-border data conflicts.
- Question: Can global firms comply everywhere?

Emerging Laws

- EU AI Act (2024 draft)—ethics in automation.
- NIS2 Directive—tougher cyber rules for critical sectors.

Organisational Liability and Due Diligence

- Organisations can be financially liable for employees' misconduct.
- Increased liability if employees are not informed about acceptable behaviour.
- Due care: Ensure employees know acceptable actions and consequences.
- Due diligence: Ongoing effort to protect others and uphold standards.

Managing Compliance

- Organisations in many countries required to comply with laws and regulations related to data protection
- organisations frequently adopt a framework of controls to manage compliance (and security):
 - COBIT (Control Objectives for Information and Related Technology)
 - COSO (Committee of Sponsoring Organisations of the Treadway Commission)
 - ISO 27002 (Code of Practice for Information Security Management)

Compliance in Information Security Goals

- Alignment with Legal and Regulatory Requirements
 - Ensure adherence to laws and regulations.
 - Maintain data privacy and protection standards.
 - Avoid legal penalties and reputational damage.
- Achieve and Maintain Trust
 - Build stakeholder confidence.
 - Demonstrate commitment to ethical practices.
- Continuous Improvement
 - Regularly update and improve security measures.
 - Adapt to evolving legal and regulatory landscapes.

Ethical Dimensions

Legal & Ethical Responsibilities in InfoSec

- As a future information security professional, you will be required to:
 - Understand the organisation's legal and ethical duties.
 - Stay updated on laws, regulations, and emerging ethical issues to reduce liabilities.
 - Educate staff and management on obligations and proper IT/security use to support the mission.

Legal & Ethical Responsibilities in InfoSec

- In addition to this, you will be
 - Entrusted with the organisation's information and systems.
 - Responsible for protection while knowing system secrets and structures.
 - Must uphold the highest ethical and moral standards.

Ethics in InfoSec

- Ethics: Study of how humans should act or rules to live by.
- InfoSec students learn ethics within a broader framework.
- InfoSec professionals need strong articulation of ethics and face greater scrutiny.

The Ten Commandments of Computer Ethics (Computer Ethics Institute)

1. Thou shalt not use a computer to harm other people
2. Thou shalt not interfere with other people's computer work
3. Thou shalt not snoop around in other people's computer files
4. Thou shalt not use a computer to steal
5. Thou shalt not use a computer to bear false witness
6. Thou shalt not copy or use proprietary software for which you have not paid
7. Thou shalt not use other people's computer resources without authorization or proper compensation
8. Thou shalt not appropriate other people's intellectual output
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans
(Source: Computer Professionals for Social Responsibility)

Detering Unethical Behaviour in InfoSec

- InfoSec personnel deter unethical/illegal acts using policy, education, and technology.
- Target three unethical behaviours: Ignorance, Accident, Intent.
- Deterrence works best via laws, policies, and controls if:
 - Fear of penalty exists.
 - Chance of being caught is high.
 - Penalty is likely to be enforced.

(ISC)² code of ethics

- The code of ethics put forth by (ISC)² is primarily designed for information security professionals who have earned one of their certifications
- This code includes four mandatory canons:
 - Protect society, the commonwealth, and the infrastructure
 - Act honorably, honestly, justly, responsibly, and legally
 - Provide diligent and competent service to principals
 - Advance and protect the profession

Ethics vs. Compliance

- Laws set floors; ethics set ceilings.
- Example: Legal surveillance—ethical if it spies on staff?

Data Governance Ethics

- **Ownership of Data:**
 - **Key Question:** Who owns data?
 - Perspectives: Users, firms, or governments?
 - Ethical considerations around control and access to data.
- **Example: Dilemma: Selling Anonymised Data**
 - **Key Issue:** Profit vs. consent.
 - Firms may monetise anonymised data, but ethical concerns arise around user consent and privacy.
 - Balancing the benefits of data utilisation with respect for individual rights.

Cambridge Analytica

- **Data Privacy vs. Political Influence**
 - Cambridge Analytica harvested data from millions of Facebook users without explicit consent.
 - Ethical dilemma: Using personal data to influence political outcomes.
- **Transparency vs. Manipulation:**
 - **Delayed Disclosure:**
 - The company delayed disclosing the data breach, raising ethical concerns.
 - Debate: Should organisations prioritise transparency over strategic advantage?
- **Implications:**
 - **Legal and Reputational Consequences:**
 - Legal actions and significant reputational damage for both Cambridge Analytica and Facebook.
 - Highlights the need for stricter data protection regulations and ethical guidelines.

Compliance in Practice

Governance Link

- Compliance = law + ethics + organisational strategy.
- Example: ISO 27001—legal alignment, ethical assurance.

Professional Dilemmas



**-Reporting breaches-
Legal duty vs. career
risk.**

- Balancing legal duty with career risks.
- Ethical responsibility vs. potential professional repercussions.

Case Study: Equifax 2017

- **Delayed Disclosure**
 - Equifax waited months to disclose a major data breach.
 - Questions raised about the ethical implications of delayed reporting.
- **Implications**
 - Legal consequences for non-compliance.
 - Reputational damage and loss of trust.
 - Highlights the tension between organisational loyalty and ethical integrity.

Strategic Challenges

- **Balancing Cost vs. Compliance**
 - Organisations face the challenge of implementing comprehensive security measures, like encryption, while managing costs.
 - Example: Encrypting all data can be expensive and resource-intensive, but it ensures robust compliance and data protection.
- **Global Operations: GDPR vs. China's Data Laws**
 - Operating globally requires navigating different data protection regulations.
 - Challenge: Aligning with stringent GDPR standards in the EU while complying with China's unique data laws.
 - Organisations may need to prioritise one set of regulations over the other, depending on their primary market and risk tolerance.

Key Takeaways

- Laws evolve—GDPR's just the start.
- Ethics challenge compliance—think beyond rules.
- Governance ties it together

References

- Lectures slides are devices from the recommended books resources.
 - Pearson Education 2014, Information Security: Principles and Practices, 2nd Edition
 - Fundamentals of Information Systems Security, by David Kim , and Michael G. Solomon



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk