

The Norfolk Cyber Conference 2024

Practical compliance in an ever-evolving world

28 November 2024

Dave Hughes

Partner

Eversheds Sutherland (International) LLP



Practical Compliance

Agenda

- Why should you listen to me?
- Practical Compliance
- Emerging Trends and Horizon Scanning
 - AI
 - Breaches
 - NIS Directive

Why should you listen to me?

Always a fair question

Practical Compliance

Why is this important?

- Sensationalist answer (to make sure people are listening):
 - no business can ever hope to fully comply with applicable privacy laws
 - there are fines of up to 4% of global, group-wide annual turnover per breach (or £17.5million per breach, if higher)
- Now that we are all terrified:
 - no business can ever hope to fully comply with applicable privacy laws, **but**
 - fines are rare in practice and, in the UK at least, typically punish deliberate non-compliance or complete ignorance or recklessness
- In addition, regulatory action isn't the key liability:
 - individual claims in an increasingly litigious area
 - reputational damage
 - time, resource and other costs in dealing with these
 - an increasing number of enforcement regimes to juggle

What is “Practical compliance”?

When it is impossible to fully comply with the law, how exactly do you decide what to do?

Practical Compliance

Principles... in plain English

1. Lawfulness, fairness and transparency

- Tell people what you are doing in advance
- Have a good, lawful reason for doing it

2. Purpose limitation

- Only use it for the purposes you collected it and said you'd use it for

3. Data minimisation

- Don't collect or retain more personal data than you actually need
- Privacy by design and default

4. Accuracy

- Make sure you keep data accurate and up to date
- Ask and audit requests for updates

5. Storage limitation

- Don't keep data for longer than you really need it
- Takes time, but have a roadmap

6. Integrity and confidentiality

- **Keep data secure and, where appropriate, confidential**
- **Act promptly when issues arise**

Practical Compliance

What does “practical compliance” mean?

- Key aims – education, understanding, efficiency and resource management
- Most common initial source of breaches / attacks
 - Human error / lack of understanding (phishing in particular)
 - IT software that isn't up to date
- What data do you hold
 - How much?
 - How long?
 - How accessible?
 - How frequently shared?
- Work backwards from these to best protect your business from the **key** risks
- You cannot eliminate breaches, but you can make them less severe, less frequent and less impactful

Practical Compliance and Emerging Trends

Most common client queries

Practical Compliance and Emerging Trends

Artificial Intelligence

- Privacy laws do not specifically deal with AI
 - AI is a form of processing so needs to be compliant with the same principles
 - if you have strong internal compliance standards you will already have solid foundations for innovation
- Recently published ICO guidance supports what we are seeing as emerging challenges
 - identification of role
 - transparency and “explainability”
 - public v private AI
 - automated decision making
 - accountability and documentation
- Privacy by design and default
 - i.e. please stop jumping in at the deep end when you cant swim

Practical Compliance and Emerging Trends

Ongoing trend of increasing cyber / ransom attacks

- Working with clients far more regularly on project management of complex, business critical incidents
- Importance of knowing your team...
 - internal and external (lawyers, forensic experts, local police contacts, insurers and other regulatory reporting obligations)...and your internal processes!
 - give yourself the most time possible to assess and determine reporting obligations to regulator(s) and affected individuals
 - the best decisions are informed decisions
- Excellent security can be undone by simple human error
 - Don't underestimate the importance of organisational security, training and education (**especially on AI!**)
 - Vast majority of client cyber-attacks are weak passwords / 2FA or failing to update IT patches
 - Common trend of supplier breaches where not sufficient due diligence undertaken (or contract is poor) – make it a differential!

Practical Compliance and Emerging Trends

Network Information Systems 2 Directive

- UK position
 - NIS(1) – OESs and RDSPs
 - If covered, comply with security requirements and self-certify
 - Report breaches of security affecting continuity of service
 - Typically caught critical infrastructure
 - New proposals due out from new(ish) Government

- EU law
 - OES/RDSP but broader scope of coverage
 - based on sector and size – including digital providers
 - extra territorial scope for those who work with the EU
 - So being UK based will not mean these will not apply
 - includes reporting obligations (in addition to privacy reqs)
 - fines of up to 2% of global annual turnover for non-compliance (or €10 million, if higher)

Practical Compliance and Emerging Trends

Network Information Systems 2 Directive

Very critical

Critical



Energy



Transport



Banking



Infrastructure for
the financial market



Health care



Drinking water



Wastewater



Digital
infrastructure



Management of
ICT services (B2B)



Government



Space travel



Postal and
courier services



Waste management



Manufacture,
production and
distribution of
chemicals



Production,
processing and
distribution of food



Manufacture



Digital providers



Research

Practical Compliance and Emerging Trends

Network Information Systems 2 Directive

- Much stricter security measures
 - Significant increase in the standards required to comply
 - Likely to require **a 22% increase in ICT budget** to comply
- Required steps likely to include:
 - duty of care to ensure security of network and information systems
 - policies on risk analysis and system security
 - policies and procedures for assessing the effectiveness of risk management measures
 - particular attention to crisis management and operational continuity in the event of a major cyber incident
 - ensuring supply chain security
 - use of cryptography and encryption

Dave Hughes

Partner

davehughes@eversheds-sutherland.com

**Eversheds Sutherland
(International) LLP**

eversheds-sutherland.com

This information pack is intended as a guide only. Whilst the information it contains is believed to be correct, it is not a substitute for appropriate legal advice. Eversheds Sutherland (International) LLP can take no responsibility for actions taken based on the information contained in this pack.

© Eversheds Sutherland 2018. All rights reserved.