EVERSHEDS SUTHERLAND

Breakwater IT Conference

Striving for practical compliance and how to respond when it goes wrong…

8 December 2022

Dave Hughes
Partner
Eversheds Sutherland (International) LLP

Practical Compliance and Breaches

Agenda

- What should you listen to this?
- What does this actually mean in practice?
- How should we respond when things go wrong?

Why should we listen to you?

The key question to start all presentations!

Practical Compliance and Breaches

Why is this important?

- Fines: **Sensationalist** answer:
  - fines of up to 4% of global, group-wide annual turnover per breach
    - or £17.5million per breach, if higher
- Fines: **Actual honest** answer:
  - Fines are rare and, in the UK at least, typically punish deliberate non-compliance or major issues relating to large global brands
- **However -** not all good news:
  - Individual claims in an increasingly litigious area
  - Reputation damage
  - Time, resource and other costs in dealing with the two above
- Requirement to report breaches to the regulator and to affected individuals (in certain cases)
  - Higher risk because you are flagging your own non-compliance to potentially those most interested in bringing enforcement action / claims against you

What the heck is “Practical compliance”?

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

Practical Compliance and Breaches

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 and Breaches

What are the requirements around breaches?

- Controller / Processor?
  - Primary obligation on Controller
  - Processor - obligation to notify the controller without undue delay of becoming aware of the breach
- Breach notification – regulator:
  - without undue delay, but not later than 72 hours of becoming aware of the breach
  - time starts on awareness
  - high risk of prejudice? – Can the business reduce that risk (with your help!)
- Breach notification – individuals
  - high risk to individuals
  - without undue delay
- Key point is that management of incident directly impacts notification, risk and liability
  - if you are not experienced, consider practicing / wargaming here

Practical Compliance and Breaches

What does “practical compliance” mean here?

- 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
- You cannot eliminate breaches, but you can make them less severe, less frequent and less impactful

What to do when it goes wrong?

(and why it always goes wrong at 4pm on a Friday)

Practical Compliance and Breaches

Recent 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
  - Vast majority of the worst cyber attacks are weak passwords / 2FA or failing to update IT patches

Practical Compliance and Breaches

Litigation Culture

- Significant increase in (spurious) litigation claims for distress
  - Often seeking between £2,000 - £5,000
  - Very difficult to defend at no cost
  - Highly frustrating to settle
- Prospect of class actions exists but remains untested (although there are EU cases being progressed as test cases, which might impact the UK)
- This means that smaller breaches might give rise to notably more liability (at least under settlement) than has previously been the case across the EU
- As with individuals rights, breaches and management of impacted individuals must be done promptly but carefully – current case study where a client was too quick to tell affected individuals and it has backfired

EVERSHEDS SUTHERLAND

Dave Hughes
Partner
davehughes@eversheds-sutherland.com
Eversheds Sutherland (International) LLP

eversheds-sutherland.com

CAM_1B-#6383288