PACIFIC INFOTECH

Cybersecurity & Compliance Rules for UK Companies

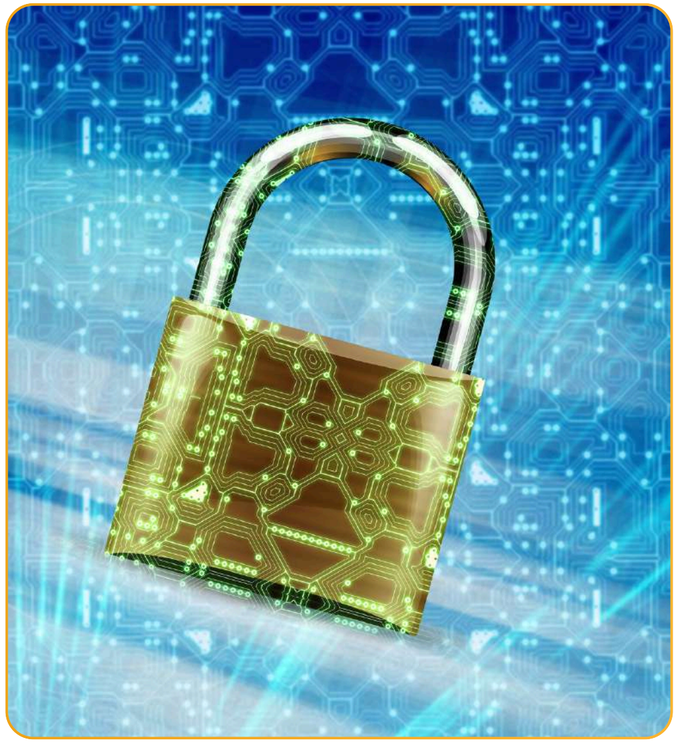
UK businesses must follow strict cybersecurity laws to protect IT systems and customer data. Failure to comply can lead to legal penalties, fines, and reputational damage.

www.pacificinfotech.co.uk

Main Cybersecurity Laws

NIS Regulations (Enforced by ICO – Information Commissioner's Office)

- Applies to digital service providers and essential infrastructure companies.
- Companies must secure IT systems against cyber threats.
- Fines for non-compliance can go up to £17 million.

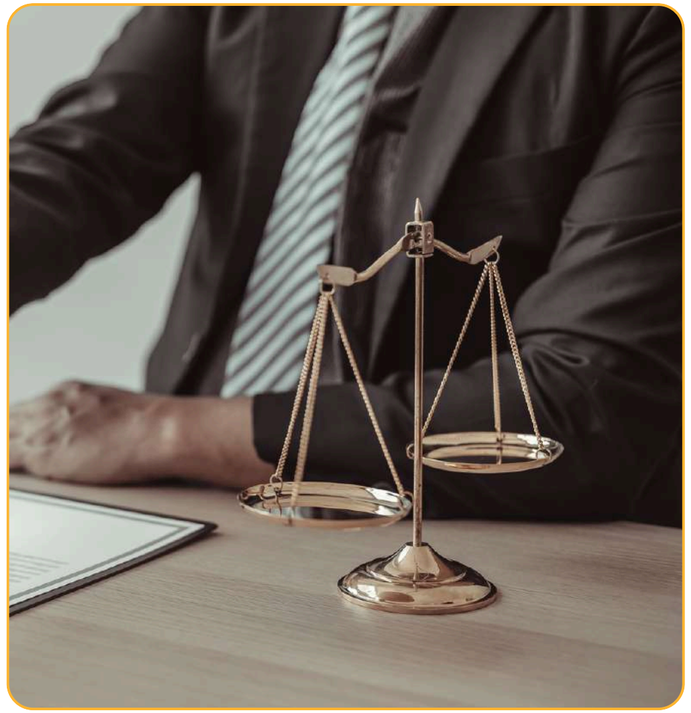


UK GDPR (General Data Protection Regulation) (Enforced by ICO)

- Companies must protect personal data from leaks, theft, or misuse.
- Failure to comply leads to huge fines and legal scrutiny.

Companies Act 2006 & FCA Regulations (For Financial & Regulated Firms)

- Financial, healthcare, and critical businesses must ensure strong cybersecurity.
- The Financial Conduct Authority (FCA) fines companies if IT failures cause data breaches.



Are Medium & Large Companies Following These Rules?

Mostly Compliant

- Medium & large businesses typically follow cybersecurity laws due to dedicated IT security teams.
- Risk of Non-Compliance

Some companies struggle due to:

- Outdated security systems that fail against new threats.
- Weak internal controls leading to data leaks.
- Lack of employee cybersecurity training, increasing cyber risks.

What Happens If Companies Don’t Follow the Rules?

Have to face heavy fines! Even big brands were not spared

Examples of Companies Fined for Weak Cybersecurity

Interserve Group Limited (Fined by ICO – May 2023)

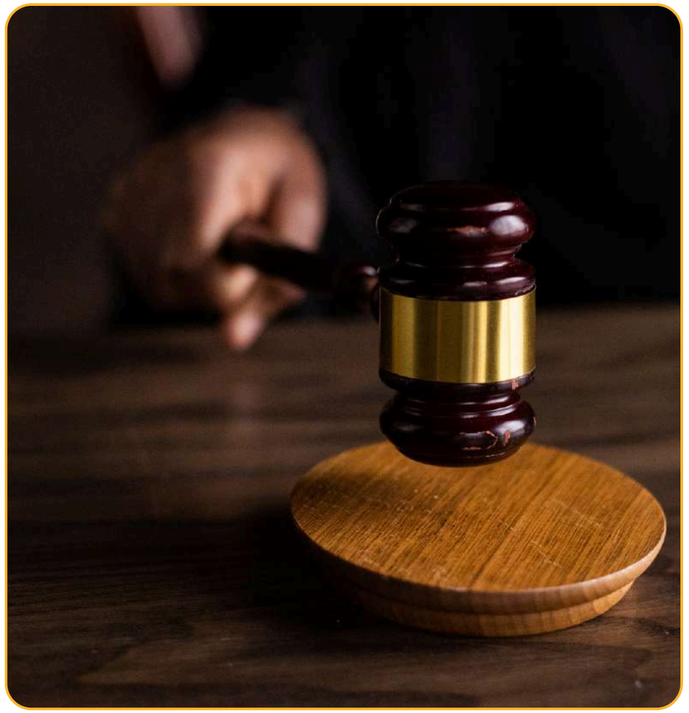
- *Fine: £4.4 million*
- *Reason: Cyber-attack exposed 113,000 employees’ data.*

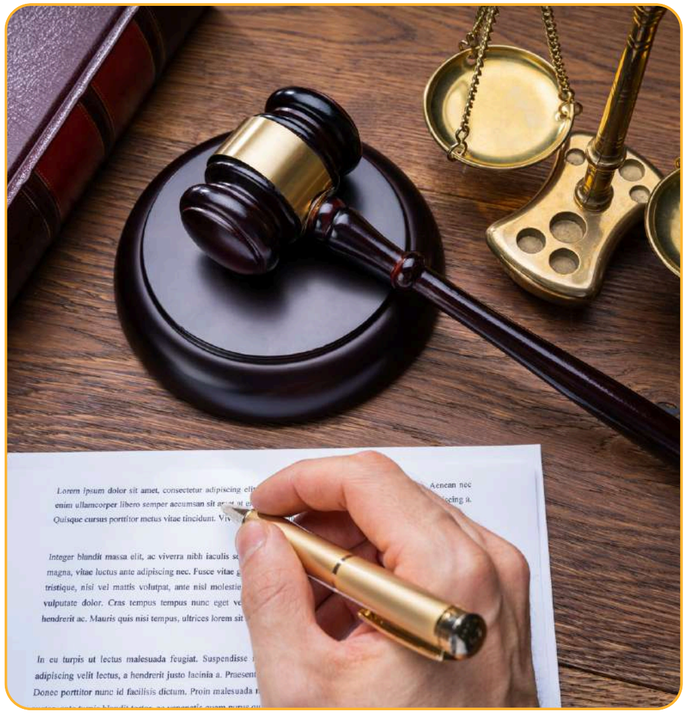
Sellafield Ltd (Fined by the Office for Nuclear Regulation – Oct 2024)

- *Fine: £332,500*
- *Reason: Failed to meet cybersecurity rules for four years.*

British Airways (Fined by ICO – July 2019)

- *Fine: £20 million*
- *Reason: Cyber-attack leaked 430,000 customers’ data.*



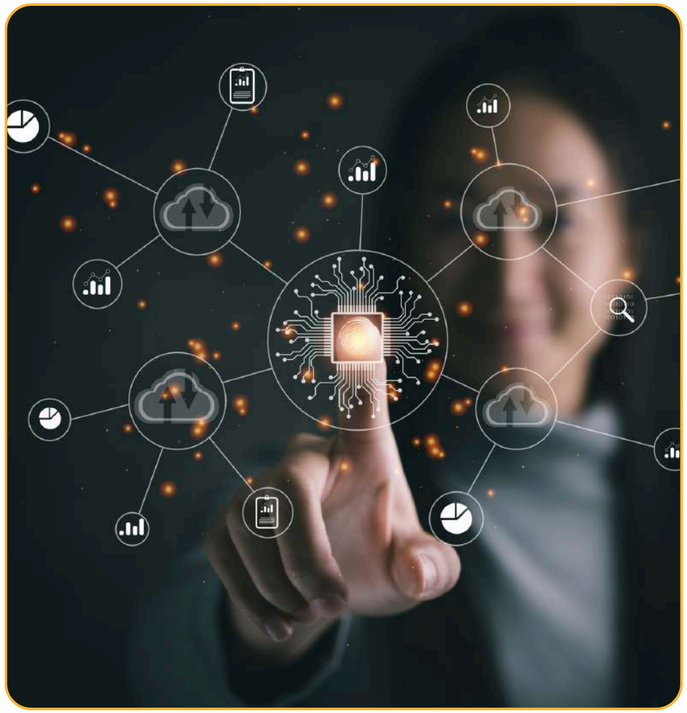


Challenges for Legal & Compliance Teams

- Rising cyber threats put pressure on legal & compliance teams.
- Teams must ensure compliance with evolving laws and manage cyber risks.
- **Responsibilities include:**
    - Regular risk assessments.
    - Strong security protocols.
    - Employee cybersecurity training.

UK Government Actions to Improve Cybersecurity

- Plans to ban public organisations from paying ransom to hackers.
- New rules may require private companies to report cyberattacks & ransom payments.



How Managed IT Services Help Businesses Stay Compliant

- Regular Security Updates – Protects IT systems from new cyber threats.
- 24/7 Monitoring & Threat Detection – Detects and stops cyberattacks in real time.
- Data Backup & Recovery – Prevents data loss from cyberattacks or IT failures.
- Compliance Assistance – Ensures businesses follow UK GDPR & NIS Regulations.
- Employee Cybersecurity Training – Helps prevent phishing, malware, and data breaches.

CONCLUSION

Cybersecurity is not optional – it’s critical.

UK laws like GDPR and NIS demand strong protection of systems and data.
Non-compliance can cost millions and damage a reputation.

Stay compliant. Stay protected.

Let experts handle your cybersecurity and compliance – so you stay focused on growth.

Thank You!

Thank You for Your Time!

Let’s secure your business together.

Contact us today for a free cybersecurity compliance check and consultation.

The Vista Business Centre,
50 Salisbury Road, Hounslow TW4 6JQ
United Kingdom

zishan@pacificinfotech.co.uk

0203 137 6707

www.pacificinfotech.co.uk