GDPR and adapting to a post-Covid world

Airmic LIVE

airmic

21 September 2021

Our learning objectives

After this session you will be able to:

- Explain the steps to reassess and reapply GDPR regulations in the today's risk environment
- Appreciate the implications for data protection laws in a post Brexit world
- Explore the ramifications in a post-Covid context including the need to adapt cyber security measures to a working-from-home (WFH) environment in order to comply with GDPR security regulations
- Consider the requirement to notify individuals following the now common ransomware attacks
- Think beyond the obvious ….

AIRMIC LIVE 22 SEPTEMBER
GDPR AND ADAPTING TO THE COVID-19 WORLD

TIM SMITH PARTNER BLM

NICK GIBBONS PARTNER BLM

SUMMARY

- Covid has accelerated changes in internet and computer use.
- These changes have resulted in a massive increase in the number of ransomware attacks.
- This combination has put stress on IT systems, IT security and cyber insurance at a time when the ICO appears to be becoming less tolerant.
- The new post-pandemic ‘normal’ will reflect many of these changes.
- Understanding the ‘new normal’ and implementing steps to address it is, therefore, an urgent priority.

CHANGES TO WORKING PRACTICES

Many of changes resulting from COVID will be part of the new normal:

- working from home for 2 or 3 days a week
- completely paperless offices
- business meetings on Zoom and Teams
- increases in online shopping and booking
- increased use of digital wallets such as Paypal
- virtual property transactions
- online doctors' surgeries
- increased use of AI

INCREASE IN CYBERCRIME

- Covid has resulted in a massive increase in ransomware attacks
- targets now include organisations and business of every type and size

> *"ransomware is the go-to method of attack for cybercriminals and the epidemic of our time."*
>
> Newsweek

ANATOMY OF A RANSOMWARE ATTACK

- Hackers typically find obvious and avoidable weaknesses in cyber security and encrypt the victim's data and cripple its computer systems.
- Recently it has also become much more common for hackers to exfiltrate personal and/or commercial data from their victims and threaten to publish it on the dark web.
- Those organisations that have effective back up systems (and there are increasing numbers that do) can restore their systems relatively quickly from those back ups.
- Those that don't will either have to pay a ransom for the de-encryption key or spend weeks trying to unlock it themselves or restore their systems with whatever data they do have.

THE COSTS OF A RANSOMWARE ATTACK

- the ransom(s)
- business interruption losses
- incident management costs
- data restoration costs
- the cost of replacement servers
- notifying individual data subjects and other businesses
- damages claims and associated legal costs

GDPR RAMIFICATIONS OF POST COVID NEW NORMAL

- Adapting cyber security measures to a working-from-home (WFH) environment to satisfy GDPR criteria
- The requirement to notify individuals following now common ransomware attacks
- The rapidly expanding data breach claims ‘industry’
- The need to review cyber insurance cover

ADAPTING SECURITY MEASURES AND A TOUGHER ICO

- The ICO states on its website that:

  "A key principle of the UK GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures"

- The new hybrid environment with many staff working from home for part of the week creates different and greater challenges, and the need for further training and supervision
- The home equipment used by staff will need to be checked or, alternatively, remote access confined to secure equipment loaned to staff by the organisation.
- The ICO has recently started to ask more searching questions in response to cyber incident reports and might in due course start fining non compliant SMEs quite regularly;

INSURANCE ISSUES

- Only some standalone cyber policies offer comprehensive cover for the consequences of a ransomware attack.

- Although, some public liability and professional indemnity policies include cyber cover, it is often very limited.

- Insurers, now faced with far more claims than they had anticipated before the pandemic are taking a tougher line with insureds whose cover is only partial or whose cover is subject to an exemption when their internet security is inadequate.

Signs that Brexit may have a significant impact on date protection law:

- A diminishing role for the ECJ
- Changes in trading patterns
- The City as Singapore on Thames
- The AUS/UK/USA IndoPacific security pact

Watch these spaces!


CLEAR ▸ CONCISE ▸ CONNECTED