THE PRICE OF SUCCESS IS LESS THAN THE PRICE OF FAILURE

ARDI KOLAH LLM
EXECUTIVE FELLOW AND PROGRAMME DIRECTOR

For further information on the GDPR Transition Programme, **click here**

Benjamin Franklin once said that 'It takes many good deeds to build a good reputation, and only one bad one to lose it.'

In many respects, one of the biggest tests organisations will face regarding reputation will be compliance with Directive 2016/679, also known as the General Data Protection Regulation (GDPR).

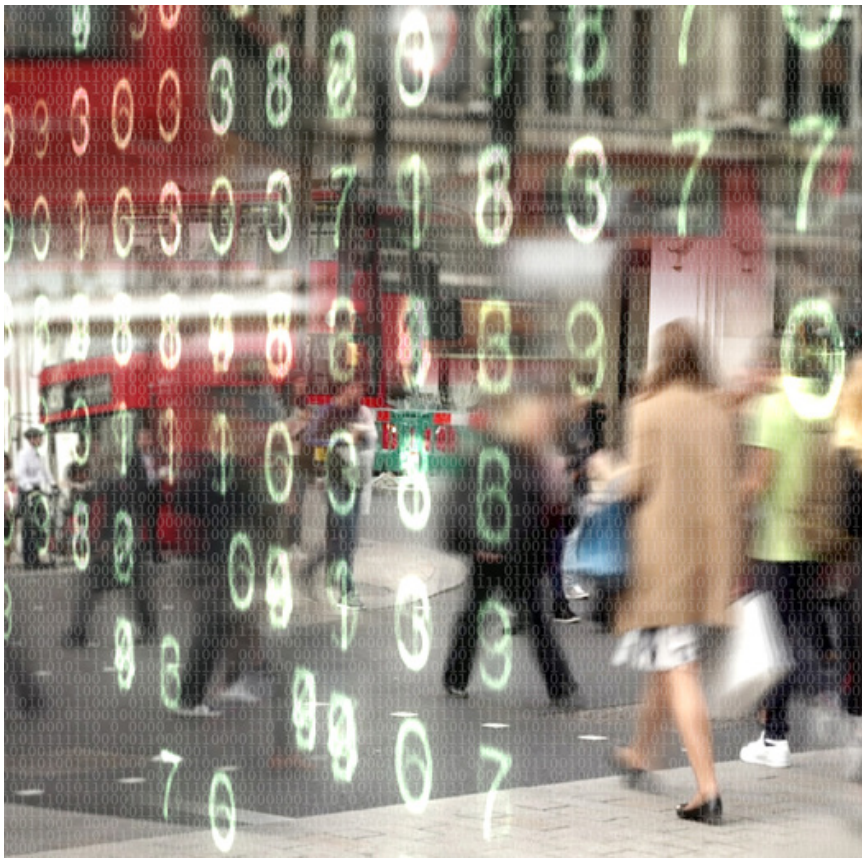
From 25 May 2018, the GDPR will be fully enforceable across all 28 EU member states. With less than 200 working days to go, many executives have just realised they are standing on a burning platform: an infringement of the GDPR can carry the highest dissuasive penalty under European law – 4% of global turnover of the preceding 12 months or €20m, whichever is greater.

A new data protection act, likely to be passed in the UK soon, will ensure that we align our data protection laws with Europe, even once we have left the EU.

So why the need for change?

It comes down to whether we can trust organisations with our personal data; the track record doesn't look good.

Only this month (July 2017), a rogue employee at BUPA stole 547,000 policyholder records, including names, dates of birth, nationalities and insurance numbers, which could all be used in scam activities. This follows the highly publicised ransomware attack



in May when 47 NHS Trusts in England reported problems at hospitals and a further 13 NHS organisations in Scotland were affected. Similarly, around half of the 40,000 Tesco Bank customers who had their accounts unlawfully accessed found that money had been removed from them. And it's not only customers or patients that fall victim. Last year, the personal data of 300,000 employees at Sports Direct were hacked.

The 2017 Cost of Data Breach Study, published by the Ponemon Institute LLC and based on research of 419 companies across 13 countries, makes compelling reading for those searching for a business case – should they need one – to accelerate plans in time for full enforcement of the GDPR.

The report calculated that the average internal cost of investigating and dealing with a personal data breach

and the aftermath of losing customers – but excluding any sanctions, fines or compensation claims – was £108 per record. And those companies surveyed were 28% more likely to suffer another personal data breach in the next 24 months.

To put this into context, the internal cost to BUPA, based on the calculations of the Ponemon Institute, would be a whopping £59m – and you can multiply this by at least a factor of 5 to cover sanctions, fines and compensation.

What should you do?

Data controllers and processors need to be put into place to ensure compliance. In the words of Elizabeth Denham, the UK Information Commissioner: 'The new legislation creates an onus on companies to understand the risks that they create for others, and to mitigate those risks. It's about moving away from seeing the law as a tick-box exercise and instead to work on a framework that can be used to build a culture of privacy that pervades an entire organisation.'

Specific skills and training are likely to be needed, as well as improvements to assurance, monitoring, PR and crisis management response practices. But by making these changes, you can turn this threat into a genuine opportunity to create, build and enhance trust amongst your employees, customers and prospects.

So if you haven't already, it would be wise to make plans to:

- appoint a data protection officer (DPO) or team
- conduct a data protection impact assessment (DPIA) 'lite'
- comply with industry codes of conduct

If you haven't yet done so, you probably need to take some professional advice in order to ensure business continuity and to reduce the risks involved with processing any personal data you may hold.

And if that sounds like an expensive exercise, just think of the costs of not doing it.

For further information on Henley's GDPR Transition Programme, **click here**

ARDI KOLAH LLM IS EXECUTIVE FELLOW AND PROGRAMME DIRECTOR OF HENLEY BUSINESS SCHOOL'S GDPR TRANSITION PROGRAMME AND EDITOR-IN-CHIEF, JOURNAL OF DATA PROTECTION & PRIVACY