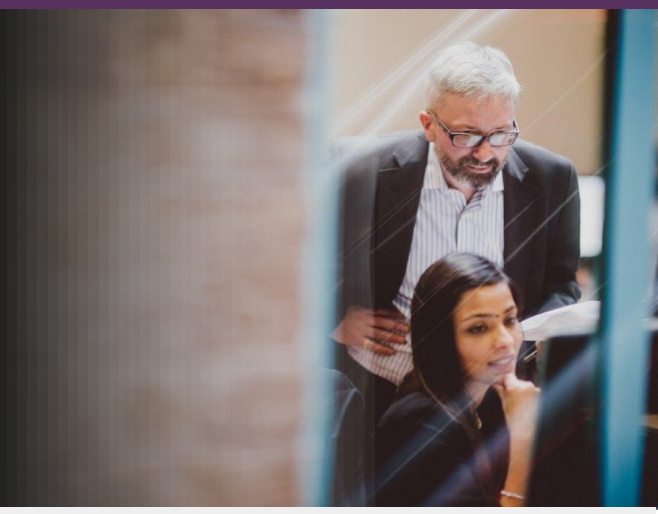
RIAA Barker Gillette

Always Available

Lockdown your data whilst working remotely

April 2020



Businesses processing personal data must keep the protection of customer and employee data at the front of continuity planning as they tackle the Coronavirus threat.

Staff are likely to be working remotely or in different circumstances which could make customer and client details more vulnerable to data breaches, and cyber-criminals are ratcheting up their fraudulent scams. It is also worth bearing in mind that data relating to employee health is likely to increase given the pandemic and extra security measures must be given to this special category of personal data.

Businesses are implementing contingency planning, with staff working from home and using domestic internet and possibly personal devices to access cloud-based software and systems, making it more important than ever to keep data safe and secure, as fines for data breaches will still apply.

Whilst it's not quite "*Stop all the clocks, cut off the telephone*", the Data Protection Act 2018 (DPA) does provide strict operating boundaries for businesses processing personally identifiable information about individuals with a statutory obligation to notify the regulator of any breach which places an individual's personally identifiable information at risk. It also gives wide ranging power to the UK's data regulator, the Information Commissioner's Office (ICO), who can impose high penalties for breaches.

Karen Cole, our Deputy Data Protection Leader and Employment Partner, explains:

"Tackling the threat of the Coronavirus is taking businesses into unchartered territory, and while data protection law doesn't stand in the way of homeworking, or the use of personal devices, it demands even greater attention to security measures, as the ones that you use in the office will need to be tailored to suit these new circumstances.

The human element is often the reason for data breaches and without direct supervision and colleagues to consult, these may be more likely to happen. Certainly, there are reports of a steep rise in attempted cyber fraud, with many more phishing emails, malware and social engineering, where fraudsters dupe staff into revealing information or making money transfers."

The other major threat to data security during the crisis is the handling of individual information about staff and visitors who have travelled to high risk areas, symptoms, test results and when self-isolation has taken place. This is personal data protected by the DPA, but where it concerns health it may be special category data under the DPA, which requires special security measures.

Such information should be collected and used only as absolutely necessary in managing risk and should not be retained unless essential, such as for an insurance claim.

Karen added:

"Ideally the management and sharing of information is set out in a policy so you know who to tell and what information is shared with whom. So, for example, the ICO has said that it is ok to inform other staff if someone tests positive, or is suspected of having contracted the virus, so as to protect the health and safety of all, but to avoid naming those individuals.

Organisations will be struggling to keep pace in this fast-changing environment, it's important to make sure you don't drop the ball when it comes to personal data. If you end up with a breach and compromised data when you

come out the other end it will be a serious issue. The ICO has the power to impose fines of up to €20m or 4% of total worldwide turnover and the damage to corporate reputation can be immense."

The ICO has published advice to help organisations in facing up to the data management challenge and while they say they will be pragmatic about matters such as speed of response to information requests during the crisis, there is no suggestion that they will accept reduced standards of data security.