GDPR and adapting to the Covid-19 world

The first Airmic-BLM white paper on the EU's General Data Protection Regulations (GDPR), released in 2018 alongside the introduction of the GDPR regulations, laid out its provisions. The second Airmic-BLM white paper – GDPR 2020 – covered the practical consequences of the regulations in the first two years of its implementation, including some of the high-profile investigations into data breaches by organisations. Since then, the world has been through at least a year and a half of the pandemic, and the Brexit transition period has ended, with implications for the state of data protection laws in the UK.

The Covid-19 pandemic has greatly accelerated domestic and business use of the internet and profoundly changed our working and social lives . This has, in turn, resulted in a massive increase in cybercrime, particularly ransomware attacks, at a time when the regulatory environment is tightening and the courts have become increasingly accommodating to individuals whose data protection rights have been breached.

Organisations that had only recently adapted to GDPR in a pre-Covid world will now need to reassess and reapply the same GDPR regulations to an already very different risk environment.

Life under lockdown has forced us all to adapt to a virtual existence lived very largely online:

- Working from home using paperless offices in the cloud became the norm.
- Similarly, internal and external business meetings have been taking place on Google Meet, Zoom and Microsoft Teams, and a growing crowd of more specialised platforms with which we have all had to become adept.
- Court hearings and mediations have regularly been held remotely.
- We became very reliant on home entertainment on sites such Netflix and Amazon Prime.
- shopping, particularly of groceries, has increased exponentially.
- Collecting one's own takeaway has been swapped for Deliveroo.
- Paper money is quickly being replaced altogether by PayPal and Apple Pay.
- While the pandemic has had many negative aspects for families, it has also given impetus to regular online family gatherings between family members, sometimes on different continents, as the older generation has been forced to become familiar with iPads and WhatsApp meetings;
- Residential and commercial property has been bought and sold on the basis of virtual viewings, without the purchaser ever stepping foot in the property.
- Children have, as well as attending online classes from their local primary or secondary school, found themselves sharing online gym, language and music classes with classmates and a teacher who might be based in (for example) Milwaukee, Brisbane or Buenos Aires.
- GPs have been swapping home and surgery visits for online consultations.

Although there will be a partial and welcome return to many pre-Covid business and social patterns, we have discovered that many of the new ways of doing things are quicker, more economic and more convenient than what we were doing before and, in some cases, enable us to do things that are simply not possible outside the virtual world of the internet.

Many of these changes are, therefore, here to stay as part of a new hybrid normal and have thrown up new technical challenges and vulnerabilities:

- Virtual Private Networks (VPNs) set up by organisations pre-Covid were frequently not built to handle such large numbers of employees working from home.
- More internet use has inevitably resulted in more human error, such as emails and other documents wrongly published or sent to the wrong email address.
- IT security teams seeking to manage a business

that previously had a known IT perimeter within an office building using the business's own secure equipment now need to control a network located in multiple different geographical points populated by staff using their own often insecure laptops, pads and smartphones – in effect, "defending the dots rather than defending the perimeter".

- Staff working from home also now use their own computer equipment for multiple different domestic, social and business activities, thus increasing the risk of error and malware infection/ hacking incidents.

- The use of different conference platforms, such as Zoom, Microsoft Teams and Google Meet, by different businesses to communicate with each other has also created risk.

These new or increased vulnerabilities have coincided with a huge increase in cybercrime during the pandemic.

Cybercrime was, until about five years ago, confined to relatively few large attacks on multinationals and government agencies. According to Interpol, the pandemic has helped cybercrime and cybercriminals to flourish:

> *"With organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption. The increased online dependency for people around the world is also creating new opportunities, with many businesses and individuals not ensuring their cyber defences are up to date. Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19."*

This increase in cybercrime has been widely reported in the national press:

> *"About 80 per cent of large companies suffer a cyber breach every year, estimates for the total annual damage from cybercrime to the global economy range upwards of $400bn."*
>
> – Financial Times

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

The types of businesses and organisations targeted by cybercriminals have become much more varied, and include small and medium-sized businesses and organisations such as schools, charities, distributors, finance companies, retailers, publishers, manufacturers, professionals, surgeries.

Ransomware attacks now also frequently involve the exfiltration of personal and commercial data. This has created additional risk and regulatory obligations, and in order businesses and organisations to sensibly evaluate sensibly the risks and regulatory obligations that they now face in the context of the new work environment, it is necessary for them to take careful account of the currently typical features of ransomware attacks:

- Hackers find a weakness in network security, such as staff who are not fully trained or who are careless, obsolete servers and/or operating systems, staff working at home on insecure devices and overloaded VPNs.

- Once in the network, the hackers gain access to the victim's data system, encrypting the data on it and causing business interruption.

- In the past year to 18 months, it has also become very common for hackers to exfiltrate personal and/ or commercial data and threaten to auction and/or publish it on the dark web.

- It is usually difficult to determine exactly what data they have taken.

- If paid, the hackers may (but do not always) stick to their side of the bargain.

The costs of a ransomware attack may include:

- the ransom

- business interruption losses

- incident management costs

- data restoration costs

- the cost of replacement servers

- the cost of notifying individual data subjects

- the cost of notifying other businesses whose commercially sensitive data may be stored on the system and damages claims by those other businesses

- damages claims by affected data subjects

- claimant and defence costs arising from third-party claims.

THE GDPR RAMIFICATIONS OF THE POST-COVID NEW NORMAL

There are also some very significant GDPR ramifications to this post-Covid new normal:

a. the need to adapt cyber security measures to a working-from-home (WFH) environment in order to comply with GDPR security regulations

b. the requirement to notify individuals following the now common ransomware attacks

c. the rapidly expanding data breach claims 'industry'

d. the need to review data breach insurance cover.

GDPR compliant cyber security and working-from-home (WFH)

WFH, even if only a part of the post-Covid normal, has rendered many existing security regimes, designed for a pre-pandemic world, redundant.

The requirements of the DPA 2018 in respect of data security are tighter than those of the DPA 1998 reinforcing the need to adapt. In particular:

a. The DPA 1998 required businesses to adopt "appropriate measures" against unlawful processing:

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, and damage to, personal data."

b. The DPA 2018 makes it a requirement that personal data must be processed in a manner that ensures appropriate security:

"Personal data must be processed in a manner that, through use of technical or organisational measures, ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage."

The ICO states on its website in respect of the appropriate security of personal data:

- *"A key principle of the UK GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.*
- *Doing this requires you to consider things like risk analysis, organisational policies, and physical and technical measures.*
- *You also have to take into account additional requirements about the security of your processing – and these also apply to data processors.*
- *You can consider the state of the art and costs of implementation when deciding what measures to take – but they must be appropriate both to your circumstances and the risk your processing poses.*
- *Where appropriate, you should look to use measures such as pseudonymisation and encryption.*
- *Your measures must ensure the 'confidentiality, integrity and availability' of your systems and services and the personal data you process within them.*
- *The measures must also enable you to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.*
- *You also need to ensure that you have appropriate processes in place to test the effectiveness of your measures, and undertake any required improvements."*

The key words in the DPA 2018 are "ensure" and "appropriate technical and organisational measures" (emphasis added).

Many of the old commonly used yardsticks and tests were devised and applied on the assumption that the majority of the workforce would be working within an office building inside an IT perimeter. The focus was, therefore, on the equipment used by the organisation within the building, security training and supervision within the office environment, and physical security measures to secure entry to the office building.

Cyber Essentials certification, for example, is primarily focused on the computer network within an organisation's building, not a five-year-old laptop on a kitchen table also used to watch Amazon Prime and communicate with friends via WhatsApp and Facebook messenger.

It is, in our view, unlikely that the ICO or a judge considering the adequacy of cyber security will be impressed by a Cyber Essentials certificate if the hacker has got into the system via a staff member working from home on an unchecked laptop.

The likely 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 designed to address this new normal.

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 need to review network security comes at a time when, in our experience, the ICO grace period following the launch of GDPR is coming to an end. The ICO is now asking far more searching questions about network security and GDPR compliance generally than was the case in the months after May 2018 when GDPR came into force.

In this regard, one of the common misunderstandings following a ransomware attack is that because the attack is primarily about a ransom, there is no need to report it to the ICO or inform individual data subjects.

- Data Protection Act 2018 (DPA) mandates notification to the ICO within 72 hours of the discovery of a personal data breach.
- The ICO stipulates that:

  "A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data."

- Individual data subjects may also need to be notified if the hackers' actual or potential access to their data represents a significant risk to them.
- Potential or actual access to commercially sensitive client data may also necessitate informing those clients even if the data is not governed by the DPA.

COVID-19, GDPR AND THIRD-PARTY CLAIMS

Covid-19 and the new normal have also coincided with more claimant friendly case law and GDPR's tougher regulatory environment resulting in many more data protection claims:

- The law has also changed significantly in the past six years:
  - Until Google and Vidal-Hall, it was necessary to prove financial loss before a court could award damages for distress. This meant that there was an easy defence to data protection claims and the numbers were limited.
  - In 2015, the Court of Appeal in Google and Vidal-Hall confirmed that the misuse of private information is a tort, and that claimants may recover damages under the Data Protection Act for distress, without also having to prove pecuniary losses.
  - In 2019, the Court of Appeal confirmed that under the DPA, damages are recoverable for 'loss of control' of data, without needing to identify any specific financial loss. The decision was appealed and we are awaiting the outcome of the hearing in the Supreme Court in April 2021.
- GDPR has both tightened regulations and raised consciousness amongst the general public about their right to make privacy claims.
- The far greater incidence of online errors and cyberattacks, and a (necessarily) tougher attitude from the ICO inevitably mean that more individual data subjects are notified about data breaches affecting their personal data.
  - A significant percentage of these invidual data subjects make damages claims.
- they are encouraged and supported by growing number of personal injury firms turning into ambulance chasing data protection claim firms backed by the litigation funding industry.

CYBER COVER AND INSURANCE POLICY WORDINGS

Faced with these changes in the internet risk environment, a review of policy cover in respect of the consequences of a cyber attacks and data breaches, including individual data breach claims, would be sensible.

Most insurers now offer a stand-alone cyber policy. Only some of these offer comprehensive cover in respect of ransomware attacks.

Many public liability and professional indemnity insurers have also adapted their policy wordings to offer some cyber and data protection cover. However, these wordings frequently offer only partial or very limited cover.

Insurers, now faced with far more claims than they had anticipated before the pandemic are being forced to take a tougher line with insureds whose cover is only partial or whose internet security is inadequate.

A thorough review of cyber security should therefore include a comprehensive gap analysis of the extent to which existing insurance cover is likely to cover today's ransomware attacks and/or staff error.

POSTSCRIPT

The pandemic has been a hard and not infrequently tragic episode. We should, nevertheless, perhaps be grateful for small mercies and reflect on what the pandemic would have been like without the internet and the capacity to survive in a virtual world while the real one was unavailable.

We now need to adapt quickly to the post-Covid world that the pandemic has generated.

UPDATES AS OF APRIL 2022

Proposals to reform UK GDPR law

In September 2021, Department for Culture, Media and Sport (DCMS) set out its proposals to reform GDPR law in the UK through its paper *Data: A new direction*, on which consultation was launched. Among the proposals are:

- To remove the obligation to: appoint a data protection officer in some cases, such as for public authorities; conduct data protection impact assessments; prepare records of processing activities.
- To create a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test (for example, in reporting criminal acts).
- A new, proposed accountability framework, where organisations will have to develop and implement a privacy management programme which includes the appropriate policies and processes for the protection of personal information. This includes the requirement to define roles and responsibilities within the organisation with respect to data protection.

These proposed reforms, which may be formally introduced at a later date, represent incremental rather than radical reforms to GDPR law. We expect that any changes to GDPR law will continue on that trajectory.

The ICO, although supportive, in principle, of increasing flexibility and reducing burdensome administrative and regulatory requirements, has emphasised the need to maintain current privacy standards and the importance of EU adequacy.

International data transfer agreement (IDTA)

The International data transfer agreement (IDTA) came into force in the UK on 21 March 2022.

The IDTA is a contract to use when making a restricted transfer of personal data to a country outside the UK, written to help organisations ensure they have the correct protections in place when transferring people's data to countries not covered by adequacy decisions.