MARSH

Adviser

JULY | 2019

Data Protection Breaches and Vicarious Liability — Considering Your Coverage Options

Adherence to data protection legislation remains a key consideration for organisations. The wide reach of data protection remains in sharp focus — in large part due to the Supreme Court granting Morrisons a right to appeal the outcome of its data breach case. The potential for employers to face far-reaching consequences in the event of a data breach currently hangs in the balance.

Data protection legislation is not a new concept in the United Kingdom (UK). The Data Protection Act 1984 introduced basic rules of registration for users of data and rights of access to that data for the individuals to which it related. These rules and rights were revised and superseded by the Data Protection Act 1998 (the "DPA 1998"). This, in turn, has now been updated by the Data Protection Act 2018, which updated our data protection laws to ensure they align with the digital age and technological advances achieved over the years. According to the Information Commissioner's Office's (ICO's) recent report on the impact of the European Union's (EU's) General Data Protection Regulation (GDPR) now one year on, there has been a significant up-tick in the reporting of data breaches (see below). And as the [1]Morrisons case demonstrates, it is essential that businesses keep pace with the increases to exposure in this evolving environment.

Employers' Liability for Data Protection — has the Exposure Increased?

The facts of the Morrisons case are that in 2014 a disgruntled senior internal IT auditor employed by Morrisons uploaded, without authorisation, the personal details of almost 100,000 Morrisons employees onto a file-sharing website, placed links to the website elsewhere on the web, and provided copies of the data to three UK newspapers. The personal details included names, addresses, dates of birth, home and mobile phone numbers, national insurance numbers, and details of bank accounts and salaries. One of the newspapers that received the personal data informed Morrisons of the data breach and it immediately took steps to ensure that the website was taken down. At the time, the ICO — the UK's data protection regulator — investigated the data breach and concluded that no action was necessary with respect to compliance with the DPA 1998, which was the appropriate data protection legislation in force at the time.

While no action was taken against Morrisons by the ICO, 5,518 of the Morrisons employees whose personal data was compromised joined together to bring the first UK class action following a data breach. Though these employees had suffered no financial loss they still sought damages from Morrisons claiming it was directly liable or vicariously liable for the criminal action of one of its rogue employees and for the distress they suffered as a result of the incident. The High Court held that whilst in these specific circumstances Morrisons was not directly liable, it was vicariously liable for the employee's actions, as they had been carried out in the course of their employment. However, mindful of the fact that Morrisons was the intended victim of the breach, the judge granted Morrisons leave to appeal. The Court of Appeal unanimously dismissed the appeal. As mentioned above, Morrisons is now appealing the decision to the Supreme Court; the outcome of this will prove pivotal for employers.

The Court of Appeal's decision gives rise to considerable concern as it leaves employers exposed to significant potential financial liability following claims from impacted data subjects for compensation caused by a data breach, even in circumstances where no wrongdoing has been committed by the organisation and that those employees deliberately intended to harm their employer. While this case was decided under the DPA 1998, following the implementation of the GDPR organisations may face an increase in the likelihood of actions in the event of a breach due to heightened public awareness. Further, the GDPR now expressly entitles individuals to claim for non-material damage (such as distress), which could increase the likelihood of claims for compensation.

Organisations should continue to focus on assessing their levels of exposure, implementing the appropriate measures to ensure that personal data in their possession is securely stored, and evaluating the effectiveness of their data breach response plans.

Note: [1] WM Morrison Supermarkets Plc v Various Claimants [2018] EWCA Civ 2339.

Understanding your coverage options — can insurance provide the "solution?"

Of particular interest in the Morrisons' Court of Appeal decision was the Court's observations on the increase in data breaches over recent years caused by either corporate system failures or employee negligence.

The Court of Appeal's decision gives rise to considerable concern as it leaves employers exposed to significant potential financial liability... even in circumstances where no wrongdoing has been committed by the organisation...

With the Court's emphasis on the role insurance coverage has to play, a key part of a company's contingency planning must be to review the extent of existing insurance cover for data protection liability, and to understand whether the cover is adequate and the limits purchased sufficient. Certain classes of insurance can provide cover for the liability and legal expenses incurred following a data breach, for example public liability, employers' liability, professional indemnity, and legal expenses. Generally, such classes of insurance only provide cover for third-party liability to pay compensation in respect of damage or distress, along with legal costs and expenses, and could be sub-limited. Such classes rarely cover the incident costs and expenses an organisation faces following a data breach — namely, the forensic costs to determine the cause and scope of the data breach, costs of notifying the affected data subjects and setting up call centres to deal with their queries, provision of credit monitoring services, and public relations costs. Even where such additional costs cover is present, it will be subject to a sub-limit and cover is typically excluded for fines and penalties.

Is a cyber policy the solution? In the Morrisons case, While the ICO investigated the incident and determined that no formal action was necessary, it is likely that Morrisons would have incurred legal costs in liaising with the ICO. Under a cyber policy, cover can be provided for the legal costs incurred in responding to regulatory requests and investigations. Further, the legal costs of defending a high court class action brought by the affected employees and pursuing a subsequent appeal are likely to be significant. Again, such costs could be covered under a cyber policy and not exposed to a sub-limit.

While there has been a focus on the finding of vicarious liability against Morrisons, particularly where it was the intended victim, when considering the application of a cyber policy this is not an area of concern. A cyber policy should respond to any legal liability an insured has for damages arising from a privacy breach — there is no distinction regarding the basis on which the finding of liability is made. In terms of the incident response expenses that Morrisons would have incurred, once it was notified by one of the newspapers of the data breach, such costs would also be covered by a cyber policy. In summary, a cyber policy provides cover for an organisation's liability arising from the unauthorised disclosure of personal or third-party information, along with litigation and regulatory investigation expenses and legal expenses. In addition, such policies may contain cover for regulatory fines, if insurable in law, and interest in the availability of such cover is increasing due to the GDPR and the potential for administrative fines.

Data protection fines and penalties — am I covered?

The GDPR introduces a two-tiered approach to the levying of administrative fines, with the nature of the infringement dictating the appropriate supervisory authority's starting point when determining the level of fine. An organisation could be fined up to €20 million or 4% of the total worldwide annual turnover of the preceding year, whichever is higher. We have seen the recent levying of a €50 million GDPR fine on Google by the French data protection authority, CNIL, for violating its obligations of transparency and failing to have a legal basis for processing personal data related to personal advertising. With the potential for such substantial fines, the question is often asked as to whether such administrative fines can be covered under an insurance policy.

Some English law insurance policies say that they will insure against fines and penalties, provided that these are insurable under the law of the policy. Under English law, fines imposed by a regulator or official body for criminal or quasi-criminal conduct cannot be covered by insurers for public policy reasons, but the position is grey in terms of civil fines. The Financial Conduct Authority ("FCA") has expressly prohibited the insurance of fines imposed by it on FCA-regulated firms; however, to date the ICO's position on the recoverability of an administrative fine for non-compliance with the GDPR has not been made clear.

In view of this continued uncertainty, in January 2019, the Global Federation of Insurance Associations (GFIA) wrote to the Organisation for Economic Cooperation and Development (OECD) requesting clarity on this point. Whilst we await the OECD's views, the position on the insurability of GDPR fines remains unclear.

How is the insurance market reacting?

Now with a requirement to notify data breaches to impacted data subjects, more data breaches are being reported in the press. In mid-December 2018, the largest collection of breached data in history was discovered – comprising more than 770 million email addresses and passwords – after it was posted to a popular hacking forum. More recently, in early February 2019, parenting site Mumsnet reported itself to the UK's data protection watchdog after an upgrade let some people see details of other users' accounts. Even where organisations take all appropriate measures to safeguard personal data, breaches can still occur, as seen in the Morrisons' case.

Brexit and data protection legislation

The EU's General Data Protection Regulation (GDPR) came into effect on 25 May 2018. The GDPR seeks to harmonise data protection laws across Europe, while at the same time placing greater obligations on organisations processing personal data, giving individuals more rights which are easier to enforce, and changing the risk profile of data protection compliance within organisations. With Brexit on the horizon will this change?

In the event that the UK leaves the EU without a Brexit deal, organisations will still need to ensure that they are compliant with data protection law. When the UK exits the EU, the GDPR will no longer be law in the UK. However, the UK Government has made clear that, to ensure the UK data protection framework continues to operate effectively in the event the UK leaves the EU without a deal, it will make appropriate changes to the GDPR and DPA 2018 prior to the UK's exit from the EU using its powers under the EU (Withdrawal) Act 2018. As such the fundamental principles, obligations, and rights introduced by the GDPR, and with which organisations and individuals are now familiar, will remain the same. Remember, the GDPR has wide extra-territorial reach and will continue to apply to data controllers or processors not established in the EU (including the UK after its exit from the EU) but where processing relates to (i) offering of goods or services (even for free) to data subjects in the EU; and/or (ii) monitoring the behaviour of data subjects in the EU.

In the event of a "No Deal" Brexit, restrictions on the transfers of personal data outside the EU will apply to transfers of personal data to the UK, which will be treated as a third country. Therefore, based on the existing guidance from the European Data Protection Board, a business based in the EU that transfers personal data to the UK will need to put in place appropriate safeguards. Unless and until the European Commission makes a finding of adequacy, standard contractual clauses represent a convenient and appropriate safeguard for most businesses.

How is the insurance market responding to the increase in such incidents? The answer to this question depends on various factors, such as the class of insurance providing the data protection liability cover, the evidence a prospective insured can provide to detail the nature and extent of the personal data held, security measures in place, and its data breach incident response planning.

Within the casualty insurance market, increases in the level of information sought from prospective insureds and a reduction in the limits available from insurers are becoming more prevalent. An increasing number of insurers have added cyber liability exclusions to remove any non-affirmative "silent" cyber risk. In addition, where data protection liability cover is provided, insurers are now applying a retroactive date of 25 May 2018, the date when the GDPR took effect. Marsh has engaged with insurers on the amendments required to ensure that existing data protection liability language is updated to take into account a policyholder's exposure to claims for compensation from affected data subjects pursuant to the GDPR and DPA 2018. Under casualty policies, this data protection liability cover in respect of third-party claims against the organisation will be sub-limited and this is expected to remain the position. Casualty insurers are increasingly viewing this as a specialist cyber risk and are greatly reducing their capacity in this field. It is anticipated that only small sub-limits will be available as this develops over the next year. It is therefore recommended that if cover is required, a separate cyber policy is purchased.

By contrast, within the cyber market, while information is also a requirement, the cyber market continues to provide cover for: the first-party costs incurred in dealing with regulatory issues; the third-party costs and damages arising from litigation following a data breach; and, where insurable, cover for regulatory fines and penalties.

ICO report: GDPR one year on

On 30 May 2019, the ICO published its report about the impact of the "GDPR one year on". The report notes the increases in personal data breaches being notified — around 14,000 personal data breach reports being received between 25 May 2018 and 1 May 2019, compared to around 3,300 personal data breach reports being received in the prior year from 1 April 2017. The ICO considers this encouraging noting that it demonstrates that "businesses are taking the requirements of the GDPR seriously". Furthermore, with nearly four times as many personal data breaches reported, the understanding of the scale of this issue for those specialising in risk mitigation also increases.

With a rise in the number of personal data breaches being reported, it is important that organisations are familiar with their insurance protection for data protection breaches, to mitigate the effects of any resulting ICO action.

The ICO report confirms it will "not hesitate to act in the public interest when organisations wilfully or negligently break the law". The ICO has said it will be "effective, proportionate, dissuasive, and consistent" in its application of sanctions, targeting its most significant powers on organisations and individuals "suspected of repeated or wilful misconduct or serious failures to take proper steps to protect person data". The ICO will use "all of the tools set out in" its Regulatory Action Policy to ensure that individual rights are upheld and that organisations comply with the law. This drive for compliance and commitment to apply sanctions is another factor for organisations to reflect on when ensuring that they have the appropriate insurance protection.

How can Marsh help you to protect against your data protection exposures?

Our risk advisory and insurance placement capabilities can assist with:

- Risk identification and exposure modelling of data and technology-related risks to create a unique profile for the organisation.
- An insurability assessment to identify the effectiveness of existing coverage arrangements against the risk profile and deliver recommendations for future treatment.
- Strong internal controls to protect customer data.
- An optimal insurance solution utilising the additional capabilities of the insurance market to deliver specific cover against privacy and technology-related exposures.

If you have any queries about any of the issues discussed in this Adviser, please contact your usual Marsh representative.

Insurance Brokers
Chartered