Risk Alert

GDPR regime will increase directors' liability

Already under attack from several directions, including ever more stringent regulatory compliance and the threat of shareholder activism, the last thing that UK company directors want to hear in the present environment is that such pressure is increasing.

Yet with the imminent arrival of the EU's new General Data Protection Regulation (GDPR) regime on 25 May, there is the very real possibility that directors and officers' liabilities for data breaches or personal data misuse in Europe will increase.

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Individuals will have the right to access and obtain data. They will have the right to request access to information held about them, to learn how it is accessed and where, the purpose of the access, and what categories of data are being accessed.

The new data regime will also see significant hikes in possible sanctions. Under existing UK legislation, the maximum fine that the Information Commissioner's Office can levy following a breach of the current Data Protection Act is £500,000. However, once the GDPR regulations come into force, the maximum fine will increase to the equivalent of €20m or 4% of annual turnover.

Cyber concerns

One key area of concern for UK company directors is that of cyber. The GDPR regime is expected to increase the liability for data breaches or personal data misuse in Europe. For example, European neighbours such as France and Italy have already taken steps to make directors liable if they fail to take reasonable measures to prevent a data breach.

Granted, there is still a degree of uncertainty as to whether the UK will follow suit, but there remains genuine concern that a case can be made, in the aftermath of a data breach, that a director gave insufficient attention to cyber security.

The areas where a company director or senior IT officer could be considered negligent and face litigation are considerable, and include:

- a vulnerable network being compromised, leading to business interruption, property damage or loss of/theft of customer data
- a data breach could result in litigation if the directors failed to ensure appropriate due diligence where data handling and/or cloud computing has been outsourced to a third party

Indeed, reliance on third party suppliers for data management will not necessarily let directors and officers off the hook, especially given that only 13% of businesses are currently setting a minimum cyber security standard for their suppliers*.

Responsibility for such oversight ultimately rests with company directors. Not only should they ensure adequate cyber security standards are set for suppliers, they should also ensure that their systems and devices are properly protected with passwords, robust fire walls, regular testing and clearly defined internal controls.

As an extra safeguard, some UK insurers have recently extended the definition of insured persons to include data protection officers under their Directors & Officers (D&O) covers, reflecting the changing needs of the market.

If you would like to know how we can help mitigate directors' liability, please contact your usual adviser.

towergate Insurance Brokers

** Source: Information Commissioner's Office*