Ascend Broking Group
Business Insurance Solutions

GDPR & Directors' and Officers' Personal Liability

Directors & Managers
Who is the risk?

This article delves into what GDPR is, who is liable, the effects on your current insurance policy and what you can put in place to protect yourself and your business.

GDPR brings in significant penalties for firms that fail to protect consumers' data. Sitting alongside it is the UK's Data Protection Act (DPA) 2018 and this states that directors themselves can be liable for criminal acts under the GDPR.

Many companies are now looking at how prepared they are for GDPR, both in terms of their data breach response plans and the personal data they already hold. Some elements of GDPR are insurable if you are in breach of legislation.

Unlimited personal liability

The directors and officers in your company are in a position of responsibility. Managers, directors and supervisors can face allegations and claims for which they may be personally liable.

Even in a company with limited liability status, personal liability is unlimited. Directors and officers are under increasing scrutiny, and it is commonplace for allegations of wrongful acts to be made.

Directors & Officers examples of claims:

A D&O defense could be for:

- *Breach of health and safety regulations*
- *Property developer agreement to purchase land for development without shareholder approval*
- *Divorced team take director vs. director action*
- *Disagreement following management buy out*
- *Company directors questioned over fatality*
- *A complicated dismissal revealed breach of the Data Protection Act*

Cyber Breach & Liability examples of claims:

A cyber incident can lead to:

- *Theft of money, data or goods*
- *Business interruption*
- *Reputational damage to your company or brand*
- *GDPR (in part)*

Ascend Broking Group
Business Insurance Solutions

Ascend Broking Group Ltd
21 Springfield Lyons Approach, Chelmsford Business Park, Chelmsford, Essex CM2 5LB
Tel 01245 449 060 | Email info@ascendbroking.co.uk | Web www.ascendbroking.co.uk

Ascend Broking Group
Business Insurance Solutions

GDPR & Directors' and Officers' Personal Liability

So what insurance protection is available?

The core purpose of a D&O policy is to provide financial protection for managers against the consequences of actual or alleged "wrongful acts" when acting in the scope of their managerial duties. The D&O policy will pay for defence costs and financial losses. In addition, extensions to many D&O policies also cover costs for managers generated by administrative and criminal proceedings or in the course of investigations by regulators or criminal prosecutors

Even if a claim isn't successful, the cover against the cost of mounting a defence will prove useful.

No organisations will be exempt, from GDPR, and staff such as senior officers should be talking to their boards to educate them about how to ensure they are in line with regulations. If they can show that they take cyber security seriously and have robust defences in place, then they are protecting their personal liability as well as helping keep the organisation secure. One way to demonstrate a commitment to security is through purchasing a robust Directors & Officer policy alongside a Cyber Breach Insurance policy which doesn't have restrictive exclusions within the wording.

Directors and officers liability insurance features

- Defence costs of health and safety, including corporate manslaughter, are included in our directors and officers liability insurance policies, meaning that should the very worst happen your costs are covered.
- Post-retirement coverage directors and officers liability insurance can include ten years' run off cover, so even after a director retires the company is still protected should a claim arise.
- Costs and awards of claims arising from pollution, a failed private offering, administration of a company pension or benefit scheme, or by individual shareholders are covered by our directors and officers liability insurance.

Who is at risk?

- Directors
- Managers
- Other officers
- Controlling shareholders

What should you do?

- Assess GDPR impact on your company
- Document a policy
- Review D&O & Cyber risk insurance policies
- Review personal liability risk with board
- Develop policies, circulate copies
- Comply with obligations
- Review third party risk and related contracts
- Have clear responsibility and reporting lines

What is not covered by a D&O policy:

- Known claims and circumstances
- Fraudulent and dishonest conduct
- Risks covered by other classes of insurance
- Insured parties suing each other
- Litigation against the company entity
- Catastrophic events for the insurer
- Claims the insurer is not permitted to cover

Who might claim against you?

Possible claimants might include:

- Shareholders
- Employees
- Creditors
- Auditors
- Customers
- Suppliers
- Regulators

Ascend Broking Group Ltd
21 Springfield Lyons Approach, Chelmsford Business Park, Chelmsford, Essex CM2 5LB
Tel 01245 449 060 | Email info@ascendbroking.co.uk | Web www.ascendbroking.co.uk

Ascend Broking Group
Business Insurance Solutions

GDPR & Directors' and Officers' Personal Liability

Directors Officers Insurance

D&O insurance policies offer liability cover for company managers to protect them from claims which may arise from the decisions and actions taken within the scope of their regular duties. As such, D&O insurance has become a regular part of companies risk management.

Companies purchase D&O cover because managers can make mistakes. D&O coverage includes financial protection for managers against the consequences of actual or alleged "wrongful acts". Policies cover the personal liability of company directors but also the reimbursement of the insured company in case it has paid the claim of a third party on behalf of its managers in order to protect them.

Coverage is usually for current, future and past directors and officers of a company and its subsidiaries. D&O insurance grants cover on a claims-made basis. This means that claims are only covered if they are made while the policy is in effect or within a contractually agreed extended reporting period, which can extend up to another 72 months or even longer in some countries.

In respect of GDPR fines coverage, if these are imposed by the regulator or official body for criminal or quasi-criminal conduct then this is not permitted under English law.

Coverage does not include fraudulent, criminal or intentional non-compliant acts or cases where directors obtained illegal remuneration, or acted for personal profit.

Download our D&O/Cyber & Professional indemnity claims comparison document at www.ascendbroking.co.uk

Cyber Breach & Liability Insurance

GDPR has increased interest in cyber insurance as there are some insurable elements of the regulations, but also for breach response support. Firms will need to inform customers if they have suffered an attack and been breached and as such, businesses should be looking to purchase well-designed policies that cover IT, legal and PR assistance during a cyber-attack.

For companies with large amounts of personal data, notifying individuals of a breach 'which is likely to result in a high risk to the rights and freedoms of individuals' will be expensive and time-consuming. These costs are insurable under a cyber policy, including follow up credit and ID monitoring.

As well as this, standalone cyber insurance will cover fines to the extent they are insurable by law. However, the extent to which insurance proceeds can be used to recoup the cost of regulator penalties under GDPR is a grey area which will need to be tested in the courts.

In terms of liability claims, anyone who suffers damage as a result of a data breach will have the right to receive compensation from the company involved. A cyber policy will cover the defence costs and liability claims resulting from a breach of confidential information.

The financial consequences of a data breach will increase the loss estimates attached to data protection on a company's risk register. Managers should examine the effectiveness of cyber policies already bought, especially indemnity limits. Whereas buyers of cyber policies would start with limits of between £100k-500k, recently new buyers have been starting with cover in excess of £5 million.

Areas where incorrect coverage could be in place:

- Is your company's data protection officer, or other GDPR-related privacy officer, a true "officer" of the company and qualifies as a covered insured?
- Are there relevant exclusions in your policy, such as regarding cyber and/or privacy?
- Are your limits sufficient to cover potential GDPR and privacy-related fines and penalties along with other costs?
- Do you know how an insurer or regulatory authority might respond to the insurability of GDPR fines and penalties?
- What is the reputation for paying claims of the insurers on your D&O & Cyber.

As privacy regulations evolve, the potential exposure to companies and their directors and officers is likely to increase. It is important to understand new requirements under these laws and how they could affect your risk profiles, and to work with your insurer to regularly review D&O and Cyber coverages to keep pace with the changes.

Contact us today for a free consultation & review

Ascend Broking Group
Business Insurance Solutions

Ascend Broking Group Ltd
21 Springfield Lyons Approach, Chelmsford Business Park, Chelmsford, Essex CM2 5LB
Tel 01245 449 060 | Email info@ascendbroking.co.uk | Web www.ascendbroking.co.uk