Article written by Alison Padfield QC, Clare Dixon and Peter Morcos of 4 New Square on 8th May 2018.

GDPR and Insurance: who picks up the tab when things go wrong?

Notwithstanding assurances from the Information Commissioner that they "*prefer the carrot to the stick*" the fact remains that the ICO will have the power under Article 83(4) the **General Data Protection Regulation** ("GDPR") to levy fines of up to €10million or 2% of annual global turnover on data controllers. Alison Padfield QC, Clare Dixon and Peter Morcos consider which aspects of GDPR compliance are likely to be insurable and/or insured, focussing in particular upon: (a) the insurability (or otherwise) of fines; (b) new potential liabilities under the GDPR; and (c) the potential pitfalls of assuming that cyber insurance will cover all civil liabilities under GDPR.

Insurability of Administrative Fines

Cyber insurance commonly excludes from cover criminal or regulatory sanctions save where they are insurable in the jurisdiction where they have been awarded. This begs the question, are ICO fines insurable in this jurisdiction?

Insurance against fines imposed for criminal or quasi criminal conduct is not permitted in this jurisdiction on public policy grounds. This is because permitting such an indemnity would all but negate the fine's deterrent effect. Consequently, such insurance, if it is entered into, is unenforceable or void. This being so: what constitutes quasi criminal conduct, and could such conduct include fines imposed by the ICO?

Lord Sumption, in his majority judgment in ***Les Laboratoires Servier v Apotex*** [2015] A.C. 430, said that an act of moral turpitude could include "*the infringement of statutory rules enacted for the protection of the public interest and attracting civil sanctions of a penal character*", and gave the example of competition law considered by Flaux J in *Safeway Stores v Twigger* **[2010] 2 Lloyd's Rep. 39.** In that case, a penalty was imposed on a company by the Office of Fair Trading, and the company sought an indemnity from its former directors and employers. Flaux J held, in refusing to strike out the claim, that the ex turpi causa principle could apply to non criminal conduct where there was a sufficient element of moral turpitude or reprehensibility, and that the penalty imposed by the OFT could engage the rule (reversed on other grounds: **[2011] 1 Lloyd's Rep. 462**, CA).

The imposition of administrative fines is governed by Article 83 of the GDPR. Not every breach will attract a fine. Issues in the balance include whether the infringement was intentional or negligent, and the degree of responsibility of the controller or processor taking into account the technical and organisational measures implemented by them. Therefore, it seems unlikely that a fine would be imposed for a wholly innocent breach.

However, when an administrative fine is imposed it is plainly intended to have an element of punitive effect with Article 83(1) stating that the imposition of fines shall be "*effective, proportionate and dissuasive"*. This suggests that it is, to adopt Lord Sumption's phraseology, a civil sanction of a penal character. Consequently, it is unlikely that fines imposed by the GDPR will be covered by insurance. This highlights the importance of insurance cover for the costs of an investigation by the ICO, with a view to minimising the prospect of such a fine being imposed.

Scope of cyber cover and GDPR

Under Article 82(1), a data subject can claim compensation for breach of the GDPR. This includes a "personal data breach", ie "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4(12)). The phrase "*a breach of security*" might be thought to suggest the involvement of a hostile external party, such as a hacker; but as can be seen from other parts of the GDPR (for instance Article 5(1)(f)), the obligation to keep data secure includes protecting it against accidental loss.

This is important in the context of current cyber policies which often insure solely against intentional cyber "attacks". Such policies are unlikely to respond to the full range of potential civil claims that can be brought under the GDPR.

Potential GDPR pitfalls for cyber cover

Even if a cyber policy offers broader cover, exclusion clauses typically found in insurance policies may produce unexpected results.

For instance, a typical terrorism exclusion clause might define a terrorist act as "*an act committed for political, religious, ideological or similar purposes including the intention to influence any government and/or to put the public, or any section of the public, in fear*".

This might for example apply to a data breach perpetrated in order unlawfully to obtain information to assist a political campaign.

What does this mean for insurers, insureds and brokers?

Policies should be reviewed to check that they provide the necessary cover both for the costs of an ICO (or other regulatory) investigation, and the full range of potential civil claims under the GDPR.

Alison Padfield QC, Clare Dixon and Peter Morcos, 4 New Square
a.padfield@4newsquare.com, c.dixon@4newsquare.com, p.morcos@4newsquare.com