Can English law insurance policies **cover fines imposed under GDPR?**

When the General Data Protection Regulation (GDPR) came into force in 2018, the headline grabber was the Information Commissioner Office's (ICO) dramatic new power to impose fines of up to €20million, or 4% of global turnover (whichever is the higher), on organisations that breached the GDPR.

One of the questions asked by policyholders in the pensions industry was whether these fines could be covered by insurance.

Many cyber liability policies are sold on the basis that they will insure against ICO fines. But the reality is that the legal position (at least in England) as to the insurability of ICO fines remains unclear. This is unhelpful for policyholders in the pensions industry, particularly as the ICO becomes increasingly active in fining organisations for data protection breaches.

The starting point is that many insurances say that they will insure against fines, provided that these are insurable under the law of the policy.

Insurance against fines imposed by a regulator or official body for criminal or quasi-criminal conduct is not permitted under English law for public policy reasons; an indemnity from an insurer would negate the fines deterrent effect. Indeed, some regulators like the Financial Conduct Authority expressly ban insurance against FCA fines.

What constitutes criminal conduct is clear. But quasi-criminal conduct? Less so.

The Court has provided some limited guidance and has referred to "infringement of statutory rules enacted for the protection of the public interest and attracting certain actions of a penal character".

So penalties or fines for quasi-criminal conduct may be regarded as involving some moral turpitude or reprehensibility by the transgressor.

An ICO fine is intended to have both a punitive and deterrent effect. The legislation sets out the matters that the ICO must take into account when considering the fine, including whether it would be effective, proportionate and dissuasive. This suggests that an ICO fine would be regarded by the court as a civil sanction of a punitive nature, quasi-criminal, designed to punish reprehensible conduct and to deter others.

So, as matters presently stand, that makes ICO fines for breach of GDPR probably uninsurable under English law.

But it could still be that fines for breaches at the most egregious (intentional or reckless breaches) end of the spectrum are regarded as punishment for quasi-criminal conduct (and therefore uninsurable). ICO fines imposed for much less serious breaches could be regarded in a different category and could still be insurable. Therefore, a case-by-case approach could emerge from the court on this issue.

These very important issues are still to be directly tested before the English Court and therefore the position remains unclear. And the ICO has refused to be drawn on the issue stating, **"a focus on insurance rather misses the point; an organisation should be looking to recognise the benefits that information rights practice to their efficiency, reputation and competitive edge".**

Therefore, for the time being, policyholders should not assume ICO fines will be covered by insurance.

By Garon Anthony, Partner, Squire Patton Boggs