Published on *The National Law Review* https://natlawreview.com

Can English law insurance policies cover ICO fines imposed on financial institutions under GDPR?

Article By:

Garon Anthony

When the General Data Protection Regulation ("**GDPR**") passed into English law on 25 May 2018, one of the headlines that heralded the new legislation was the Information Commissioner Office's ("**ICO**") new power to impose fines of up to €20million, or 4% of global turnover (whichever is the higher) on organisations that breach the GDPR.

And, given the dramatic increase of the ICO's power to impose fines, one of the big questions asked by insureds, brokers and insurers was whether the fines could be covered by insurance?

The question was repeated earlier this month following on from the announcement of the fine of €50million imposed on Google by the French data regulator for breach of GDPR.

Some answers may soon be available, if only in part.

The Global Federation of Insurance Association has earlier this week called on the OECD for clarity, saying, *"there is international confusion as to the insurability of fines and penalties. OECD work to clarify this issue would benefit consumer and insurer contract certainty*". The OECD has responded

by saying that it will now look at the issue and guidance could be forthcoming in the near future.

But for now, the position at least under English law as to the insurability of GDPR fines remains unclear. That is (to say the least) unhelpful for all participants in the insurance market, particularly as the ICO becomes increasingly active with fining organisations for breaches of data protection law.

The starting point here is that many English law insurance policies say that they will insure against fines and penalties, *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 deterrent effect of the fine). Indeed, the Financial Conduct Authority ("**FCA**") expressly bans the regulated commmunity from insuring against FCA fines for misconduct.

What is 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*" (per Sumption LJ in *Les Laboratoires Servier v Apotex*[2015] AC 430). 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 under GDPR *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.

As matters presently stand therefore, 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 the issue.

These very important issues are still to be directly tested before the English Court and therefore so the position remains unclear. OECD guidance in this regard would certainly be welcome (albeit not in any sense binding on the English Court), particularly as the ICO has refused to be drawn on the issue. Last year the ICO said that this was not a matter for the ICO and that *"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 moment, the message to policyholders is not to assume ICO fines will be covered by an English law insurance policy. But value is clearly still to be found in such policies when it comes to, for example, insuring the costs of responding to a data breach or cyber-attack, dealing with related third party claims and complaints and repairing damaged software.

National Law Review, Volume IX, Number 25