CLYDE&CO

THE INSURANCE HUB

JANUARY 30, 2019

# Insurability of fines and penalties for breaches of the GDPR: A UK and German perspective

The increasing powers of regulators, together with the heightened focus on corporate governance and individual accountability, means that companies and their directors and officers are increasingly exposed to investigations which may lead to the imposition of fines and penalties. The question of whether these fines are insurable is one which (while not new) has been brought into sharp relief by the introduction of the General Data Protection Regulation. In this article, we examine this question from the perspective of the UK and Germany.

The increasing powers of regulators, together with the heightened focus on corporate governance and individual accountability, means that companies and their directors and officers are increasingly exposed to investigations which may lead to the imposition of fines and penalties. The question of whether these fines are insurable is one which (while not new) has been brought into sharp relief by the introduction of the General Data Protection Regulation (GDPR), under which supervising authorities (the Information

Commissioner's Office (ICO) in the UK and the Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) and the various state level Landesbeauftragte für den Datenschutz (LfD) in Germany) can, amongst other things, impose fines of:

- up to €10million or 2% of annual global turnover, whichever is higher, for breaches of provisions of the GDPR, such as the obligations on data controllers and data processors;
- up to €20million or 4% of annual global turnover, whichever is higher, for breaches of the provisions of the GDPR, such as the principles for processing, the conditions for consent and the rights of data subjects.

It is worth noting that not all infringements of the GDPR will lead to the large fines that have captivated the press. Whilst there has been the recent €50 million fine imposed on Google by the French data regulator, CNIL, for "*lack of transparency, inadequate information and lack of valid consent regarding ads personalisation*", the 41 fines that have thus far been imposed in Germany have largely been low value, with the highest fine being in the amount of €80,000. The UK has yet to issue significant fines, though an enforcement notice has been issued to the Canadian company AggregateIQ Data Services ("AIQ"), as part of a wide-ranging investigation by the ICO into the improper use of personal data analytics for political purposes (involving Cambridge Analytica and Facebook), which may, in time, lead to a significant fine under the GDPR.

The question is: will GDPR fines be insurable? There is a huge degree of uncertainty on this point, an uncertainty which has recently led the Global Federation of Insurance Associations to call for clarity from the Organisation for Economic Cooperation and Development (OECD) about whether insurers can pay out for fines imposed under the GDPR - not a declaration one way or another, but a guide on how different supervisory authorities will consider the issue.

Until such clarity comes, we examine the question of insurability in this article from the perspective of the UK and Germany.

## Insurability of fines and penalties

As a preliminary point, it should be noted that the UK and German authorities have not themselves declared whether or not any fines they issue should be capable of being insured, unlike, for example, the Financial Conduct Authority (FCA) in the UK, which expressly prohibits the insuring of fines it imposes for breaches of financial regulations. Therefore, we must first consider general principles, which can then be applied to the GDPR.

The first port of call is the policy language. Under some wordings, there is no coverage for any fines and penalties whatsoever but, under other common formulations, only criminal fines are excluded and fines are covered to the extent they are "insurable by law". If it is not "insurable by law" then the courts will consider it void and unenforceable.

In the UK, whether an insurance policy will cover a fine imposed by the ICO following, for instance, a data breach, depends on the public policy question of whether it is possible to recover for a loss which results from your own wrongdoing. This statement, often expressed in the Latin maxim *ex turpi causa* and known as the "illegality defence", is a well-known common law public policy doctrine (based on the *ex turpi causa* dictum of Lord Mansfield in *Holman v Johnson* (1775)). In the insurance context, the making of an insurance claim for the recovery of fines imposed on companies and individuals for illegal acts would remove the deterrent effect of such fines; the "illegality defence" prevents this. After many conflicting cases as to how to apply the illegality defence, the Supreme Court in *Patel v Mirza* [2016] UKSC 42, laid down the factors that should be taken into account when deciding whether it would be in the public interest to enforce a claim

despite some "illegality" on the part of the claimant:

1. the underlying purpose of the prohibition which has been transgressed;
2. any other relevant public policies which would be rendered ineffective or less effective by the denial of the claim; and
3. the need for proportionality

There are three broad categories of conduct for which any fine or penalty might be imposed:

- intentional or reckless wrongdoing;
- strict liability situations, where no particular fault is required; and
- negligence.

Broadly, the position in the UK is as follows:

- Fines resulting from intentional wrongdoing will not be indemnifiable whatever the type of fine, and might also, in any event, be excluded by other policy provisions, such as fraud or dishonesty, or personal advantage exclusions. However, where the fine is "indirect", a company might still be able to recover from a director a corporate fine resulting from intentional conduct, if the company can show it was only vicariously liable for that conduct (leading to complicated questions of attribution). The Court of Appeal in *Safeway v Twigger* (2010) said that, in that case, the issue of attribution was irrelevant as the fine was personal to the company – the offence was not one which could be committed by an individual (including the directors). This could be contrasted with other statutory provisions which contain criminal offences which can only be committed by individuals.
- Strict/no fault liability fines will likely be indemnifiable, as there is no requirement that the insured's conduct involves an element of moral turpitude (subject to the caveat that fines imposed by certain regulators, such as the FCA, mentioned earlier, are uninsurable in all cases).[1]
- Fines imposed for negligent conduct are more complicated. Civil fines or penalties imposed for purely negligent conduct should, in theory, be insurable. In *Safeway*, the Court of Appeal concluded that for the illegality defence to apply there must be an element of moral turpitude or moral reprehensibility involved in the relevant conduct. In the subsequent Supreme Court case of *Les Laboratoires Servier v Apotex Inc* (2014), the court supported this by stating, "*... non-criminal acts giving rise to the [illegality] defence includes cases of ... the infringement of statutory rules enacted for the protection of the public interest and attracting civil sanctions of a penal character, such as the competition law considered by Flaux J in Safeway Stores Ltd v Twigger ...*" Further, in *Sainsbury's Supermarkets Ltd v MasterCard Inc and ors* (2016), the Competition Appeal Tribunal further held that, "*whether an infringement of competition law can trigger an illegality defence depends upon whether that infringement is an "innocent" one (in which case, we consider it cannot) or a "negligent" or "deliberate" one (in which case it may do).*" As such, the *ex turpi causa* principle is engaged by conduct which reaches a certain level of moral turpitude falling short of criminal behaviour. If it is engaged, the fines are not insurable, if it is not, then they may be insurable. An assessment will therefore need to be made as to the degree of moral turpitude involved in the conduct leading to the infringement.

In Germany, it is still not decided whether, and to what extent, fines and penalties are insurable. The decisive legal test, as in the UK, will be whether it is in breach of public policy. The German Civil Code, section 138(1), states that any legal transaction which is contrary to public policy is void. Arguably, the insuring of fines generally contradicts public policy as the coverage of fines can impair the preventative purpose of the fine. Furthermore, it is considered that the insuring of fines interferes with the effectiveness of the regulation if the threatened fine is covered by an insurance policy.

However, some scholars and authors distinguish, in particular, between fines for intentional conduct and those for negligent offences, arguing that the civil law should only sanction a behaviour that is also punishable under criminal law and, therefore, intentional. Accordingly, negligent conduct may be insurable under this reasoning.

However, the prevailing opinion in Germany, in the absence of authority on the point, is that the coverage of fines is contrary to public policy and there are many indications that the coverage of fines and penalties under German law is void. If so, providing such coverage would primarily lead to the unenforceability of the respective insurance claims and might also lead to regulatory action by the German supervisory authority, the Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).

Also, in Germany, there may be a distinction to be made where there is no negligence or intentional wrongdoing by the entity personally, as opposed to liability of the entity for acts by management which have caused the entity to be in breach of the GDPR. Section 103 of the German Insurance Contract Act (VVG) provides that the insurer shall not be obligated to effect payment if the policyholder has intentionally and unlawfully caused the loss suffered by the third party. This wording does not specify where the intent of the policyholder has to come from, but it is established in case law that this provision takes intent to mean the intent of the management and higher of the company. Could an inference therefore be drawn from Section 103 to assist with addressing the question of the insurability of fines where culpability is placed on management and higher? This is yet to be addressed by the German courts.

## How does this analysis apply to GDPR fines?

Fines flowing from criminal conduct will not be insurable as it is clearly against public policy for fines resulting from intentional/reckless criminal wrongdoing to be indemnifiable. In the UK, for example, fines imposed in relation to the two new criminal offences of (i) intentionally or recklessly re-identifying individuals from anonymised data, and (ii) altering records with the intention of preventing disclosure of that information pursuant to a subject access request (introduced into the Data Protection Act 2018 (DPA 2018) by way of the GDPR's permitted derogations), will not be insurable. [2]

How administrative fines under the GDPR, however, will be addressed is less clear.

When deciding whether to impose an administrative fine, as opposed to an alternative enforcement measure such as a reprimand, one of the key considerations regulators shall have regard to under the GDPR (as set out in Article 83(2)) is the intentional or negligent character of the infringement. This is alongside factors such as the severity and duration of the data breach; whether the company has had a previous data breach; the type of personal data involved in the breach and whether the breach affects the rights and freedoms of the individuals affected.

Clearly intentional conduct (which is not necessarily criminal) will be uninsurable for offending public policy both in the UK and Germany. It is our view, however, that it can be strongly argued that a GDPR fine may be insurable if the conduct was negligent and the degree of negligence leading to the infringement was low on the moral reprehensibility scale. In the UK, the *Safeway* decision supports this position and whilst there is no equivalent case in Germany on this point, it is our view that section 138 of the German Civil Code is open to interpretation and negligent conduct on the lower end of the scale may not be held to offend public policy and thus be capable of being insured.

With regard to the largest fines that may be imposed, it may be that, in practice, they will only be issued in the most egregious of cases where there is a clear intentional conduct, such that the question of insurability is moot on the basis that these cases are clearly against public policy and thus uninsurable. But it is our

view that the position is not clear cut as regards cases not involving intentional conduct and it is not sufficient to say conclusively that GDPR fines will never be insurable in the UK or in Germany.

Further, insurance will still play a part, responding as it may do to investigation costs, defence costs, and breach response costs, depending on the policy in question. These costs could well be significant and public policy concerns would generally not preclude coverage for such costs.[3]

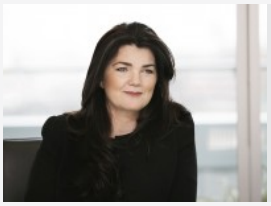
Where does this leave insurers? For the time being it remains to be seen how this will be dealt with on a European level and we are left with uncertainty and little guidance from regulators. The ICO has said that "*a focus on insurance rather misses the point, and organisations should be looking to recognise the benefits of good information rights practices to their efficiency, reputation, and competitive edge*." German regulators, too, have stated that they aim to educate and assist entities to comply with the GDPR regime, especially smaller entities, and that fines are not the focus. As the OECD remit is only to provide a guide on the approaches of the different supervisory authorities and in lieu of these issues being examined by the courts, certainty may be a way off.

[1] In *Geddes (D) (Contractors) Ltd v Neil Johnson Health & Safety Services Ltd* [2017] CSOH 42, a Scottish case, the court held that an insured may be entitled to indemnification for strict liability criminal fines or regulatory financial sanctions.

[2] These offences will incur unlimited fines and may be 'reportable' offences (i.e. they may be included on a criminal record check). Where an offence under the DPA 2018 has been committed by a company and it is proved that it has been committed with the consent or connivance of, or is attributable to neglect on the part of a director, manager, secretary or similar officer, or person purporting to act in such a role, that person is also guilty of the offence and liable to be proceeded against and punished accordingly.

[3] *Ex turpi causa* principle does not apply to indemnity for the costs and expenses of defending an action brought by a third party: *Coulson v News Group Newspapers Ltd* [2012] EWCA Civ 1547

## Authors

Helen Bourne
Partner

Dr Henning Schaloske
Partner


## More by the authors


Europe is waking up to the need for effective class actions

Germany introduces model declaratory action law

Insurance predictions 2018: Dieselgate, kill or cure for German D&O?
Smart data will transform insurance service provision
FI and D&O International Review - July 2017

## Categories

Market insight | Cyber