The Legal 500 Country Comparative Guides

Hot Topic

Insurability of GDPR Fines in Austria - Yet another “Moral Hazard” Debate?

Contributing Firm
Vavrovsky Heine Marth Rechtsanwälte

Authors
Philipp Strasser
Partner
philipp.strasser@vhm-law.at

Jan Philipp Meyer
Attorney at Law
Jan.Meyer@vhm-law.at
Insurability of GDPR Fines in Austria - Yet another “Moral Hazard” Debate?

The European Union’s new data protection regime – the General Data Protection Regulation (EU) 2016/679 (“GDPR”), which replaced its 20-year-old predecessor – attracted international attention even beyond the EU’s borders in recent months. In fact, few other instruments of secondary European Union law have been more widely received and discussed than the GDPR. The reasons behind this increased public interest for this regulation are manifold.

One of the more controversial issues in the colourful GDPR discussions of recent months involve the regulation’s provisions on administrative fines. In case of data protection infringements, the competent data protection authority may impose fines of up to either EUR 20 million or - if that figure is higher – up to 4 % of an undertaking or group’s annual turnover. According to the regulation’s recitals, one of the main reasons for the comparatively drastic level of fines is the European legislator’s desire to “strengthen the enforcement” of the GDPR’s rules.

Understandably, the possible subjects of such fines - both companies and organisations as well as the executives acting on behalf of them – posed the question of who would ultimately bear these fines and any other financial consequences associated with (alleged) non-compliance.

Consequently, insurers have stepped in and started offering insurance coverage with regard to GDPR infringements, with some of the underlying insurance conditions expressly limiting coverage to risks considered insurable by the applicable substantive law. Thus, while the scope of cover available on the market differs in detail, the crucial question is, whether and, if so, to what extent such risks are insurable in the first place. In other words: Will the financial burden ultimately be borne by the person or entity in infringement of the GDPR or can it, in a legally binding manner, be passed on to an insurer? This article takes an Austrian perspective on the issue.

Insurability of (GDPR) Administrative Fines - A Mere Question of Balancing of Interests?

The question of whether and to what extent the consequences of GDPR non-compliance are insurable is not regulated at European Union level. It is, to a large extent, closely linked to the classic “Moral Hazard” debate, ie the influence that active insurance cover has on an entity’s behaviour.

Looking at the specific example of fines to be issued in a GDPR context, the question could be rephrased as follows: Would data controllers and data processors display less risk-adverse behaviour when handling personal data if the financially negative results of their actions were ultimately to be borne by an insurer? Provided that the insurance premiums are economically viable, the questions will most likely be answered in the affirmative.

At the same time, regard is to be had to the purposes of monetary fines in general and administrative fines in the GDPR context in particular (cf below). One of the more obvious
purposes of monetary fines lies in their punitive nature and, thus, the desired dissuasive effect.

Bearing in mind these (desired) purposes, the question of insurability boils down to a question of legal policy. Does the legislator recognise situations, in which an individual’s need for insurance coverage outweighs the interests of the general public in ensuring compliant and lawful conduct by all market participants?

**European Trend on Insurability of GDPR Fines.**

Due to the absence of an established European rule or standard, the question of insurability is to be determined individually by the member states. As has been noted, this determination individual to the different national jurisdictions primarily involves a balancing of interests. Can the desired effect – dissuasiveness of an administrative fine – take a back seat to the need of the potential insured to be protected from the radical effects of such fine or other consequences of non-compliance? And if so: To what extent?

Due to various differences of the legal concepts relied upon by the different national regimes, it is hard to make out a definite “European trend” on insurability in this regard. Nevertheless, from a broad perspective, one trend can be observed: Most member states seem to be sceptical towards the insurability of GDPR fines and less sceptical towards the insurability of associated costs. In some countries, this scepticism is due to the general principle that all administrative fines are considered as being uninsurable per se – mostly for reasons of public policy, ie stipulating such insurance contracts as being immoral. Only a select few member states seem to allow for a (partial) insurability of GDPR fines.

In contrast, as far as other costs associated with data protection violations, such as legal fees, public relations costs, damages or compensation to be paid to affected data subjects or possible recourse claims by the organisation against its management, the room for insurability, on the European spectrum, seems significantly broader.

Needless to say, the global insurance market has not taken a mere observant role, leaving the business decisions to the EU member states’ policy considerations as regards insurability. In fact, insurance undertakings have already come up with ways and means to circumvent public policy hurdles by offering insurance coverage from outside of the EU (eg via Bermuda, Singapore, and Mexico). Some of these countries are already relied upon as underwriting jurisdictions for insuring other punitive fines issued in the EU or the United States of America.

**General Conditions for Imposing Administrative Fines Set by the GDPR**

The text of the GDPR sets out general principles and conditions directed at the national supervisory authorities on imposing administrative fines. This provision is supplemented by explanatory notes contained in the regulation’s recitals. In addition, the so-called Article 29 Data Protection Working Party (now named “European Data Protection Board”) issued guidelines on the application and setting of GDPR fines in October 2017.

The GDPR’s core principles for imposing administrative fines are set forth in Article 83 of the regulation. According to Article 83 para 1 GDPR, the imposition of administrative fines shall
“in each individual case be effective, proportionate and dissuasive”. Consequently, when issuing fines, the national supervisory authorities are required to take into account the individual circumstances and to evaluate, whether a fine should be imposed in addition to or instead of other administrative measures. Such other measures – the supervisory authorities’ so-called “corrective powers” – are regulated in Article 58 para 2 GDPR and may include issuing warnings or banning data controllers from processing personal data.

The criteria for this proportionality test are set forth in Article 83 para 2 GDPR. According to that provision, regard is to be had to, inter alia, the nature, gravity and duration of the infringement, the degree of responsibility, actions taken to mitigate the damage, the established compliance system before the infringement (eg adherence to a code of conduct) and aggravating factors like financial benefits gained from the infringement.

**Administrative Fines under Austrian Law - Underlying Principles**

Monetary penalties such as administrative and criminal fines are regulated, on a general level, by the Austrian Administrative Penal Act (Verwaltungsstrafgesetz) and the Austrian Criminal Code (Strafgesetzbuch). These general provisions are supplemented by a number of national and international statutory provisions.

In the context of this article, the Austrian Data Protection Act (Datenschutzgesetz) is of particular relevance. This act, which supplements the provisions of the GDPR, was recently amended. It, inter alia, further specifies the requirements and procedures for imposing fines; additionally, it provides for administrative fines in connection with data protection infringements not regulated by the GDPR. Section 30 of the Austrian Data Protection Act provides that the competent supervisory authority, the Austrian Data Protection Authority (Datenschutzbehörde), is only competent to issue fines vis-à-vis legal persons. In contrast, the GDPR generally allows for fines also to be issued against individuals.

While the legal qualification of the fines provided for in Article 83 GDPR still have to be clarified for some European jurisdictions, the Austrian legal system qualifies them as administrative fines within the meaning of the Austrian Administrative Penal Act. This legal assessment has been confirmed expressly in a paper issued by the Austrian Data Protection Authority.

**Administrative Fines under Austrian Law - Insurability**

Austrian law does not explicitly prohibit the granting of insurance cover for administrative or criminal fines. However, contracts stipulating the refund of fines issued in connection with future offences or infringements are considered immoral due to the moral hazard of undermining the desired punitive and preventive effect of such fines. Consequently, the Austrian Supreme Court found ex ante-indemnity agreements to be void.

In contrast, a contract entered into after the offence has been committed is not regarded as immoral as such. However, even these agreements may be invalid if the offender is reimbursed even where the infringement was intentional, as such undifferentiated reimbursement of fines could constitute an inducement or reward for deliberate violations of the law.
The same legal reasoning applies to situations where such agreements concern fines to be issued vis-à-vis legal entities and these fines, too, are punitive and preventive in nature.

Thus, monetary fines such as those provided for in Article 83 GDPR are not insurable in Austria. For this reason, many GDPR-related insurance products available on the Austrian market contain clauses which substantively stipulate that “fines (and recourse claims out of fines) are covered, as long it does not infringe statutory provisions”.

**Recourse Claims against Executives under Austrian Law - Panacea D&O Insurance?**

Considering the above, a follow-up-question comes to mind. Can a legal entity assert recourse claims against (former) executives liable for the underlying infringement? And if so, are these recourse claims insurable under Directors’ and Officers’ Liability Insurance policies (“D&O insurance”) or similar insurance products covering pecuniary losses (Vermögensschäden) such as Cyber Security products?

Given the fact that the GDPR has become applicable only a few months ago, this issue has not yet been decided by the state courts. The prevailing opinion in literature is that such recourse claims are - if at all admissible - not insurable under Austrian law.

First, scholars and practitioners have pointed out a number of convincing reasons against the possibility for a legal entity, ie the addressee of the fine, to pass on the financial loss to the acting executives (and, in theory, the D&O insurer involved).

The grounds given for this scepticism towards the admissibility of passing the risk on include the legislator’s express and deliberate decision to address the entity (and its shareholders) instead of the responsible individual. In fact, the involvement of an entity’s shareholders may prove to be more advantageous as regards the desired strict enforcement of the GDPR than a mere extension of the duties already imposed on the entity’s executives. Keeping in mind that, as a rule, the GDPR stipulates for fines to be issues vis-à-vis the entity (and not the executive), it seems all the more comprehensible to oppose a passing on of the risk. If such passing on to an individual (or its insurer) were possible in general, this would undermine the desired dissuasive, steering effect. Thus, there is a strong case against the admissibility of a passing on of the risk.

Second, even if – contrary to the above indication – Austrian courts were to find such recourse claims to be legally admissible, these claims would, in any case, not be insurable under Austrian law. Irrespective of the question whether an administrative fine can be qualified as a pecuniary loss under Austrian law in the first place, the above remarks on the immoral nature of agreements stipulating a reimbursement of monetary fines issued based on violations of the law have to be borne in mind. The intended behavioural incentives inherent in the GDPR and other legal instruments providing for legal consequences of unlawful conduct – namely the entity’s obligation to ensure compliant and lawful conduct throughout the entire organisation, eg by establishing a Corporate Compliance System – would be undermined if the risk were ultimately borne by an uninvolved third party.

It should be pointed out that the above remarks concern the insurability and passing on of the
administrative fine only. A more liberal assessment may apply to related expenses such as legal
fees or public relations costs incurred by the entity or the insured person. In this respect, the
granting of (provisional) insurance cover would seem less problematic. In general, Austrian law
allows for an insurability of both defence costs as well as damages under civil law (cf Art 82
GDPR). The Austrian Supreme Court explicitly confirmed the insurability of these cost items
and affirmed that the preventative and punitive purpose of the fine (making the fine itself
uninsurable) does not extend to these related expenses.

Obviously, such confirmation of coverage must exclude insurance payments in case the
violation of law, in the end, turns out to have been committed consciously or even intentionally.

Conclusion

GDPR fines and respective recourse claims are not insurable under Austrian law. The Austrian
legal system qualifies agreements providing for the opposite immoral and thus void because
such agreements entail undesirable situations where the burden of the infringement, the fine,
would ultimately be borne by the insurer, an uninvolved third party, instead of the wrongdoer.
This, in turn, would create incentives for unlawful behaviour – a “Moral Hazard”. Some costs
incurred in relation to an (alleged) GDPR-infringement may, however, be insurable.