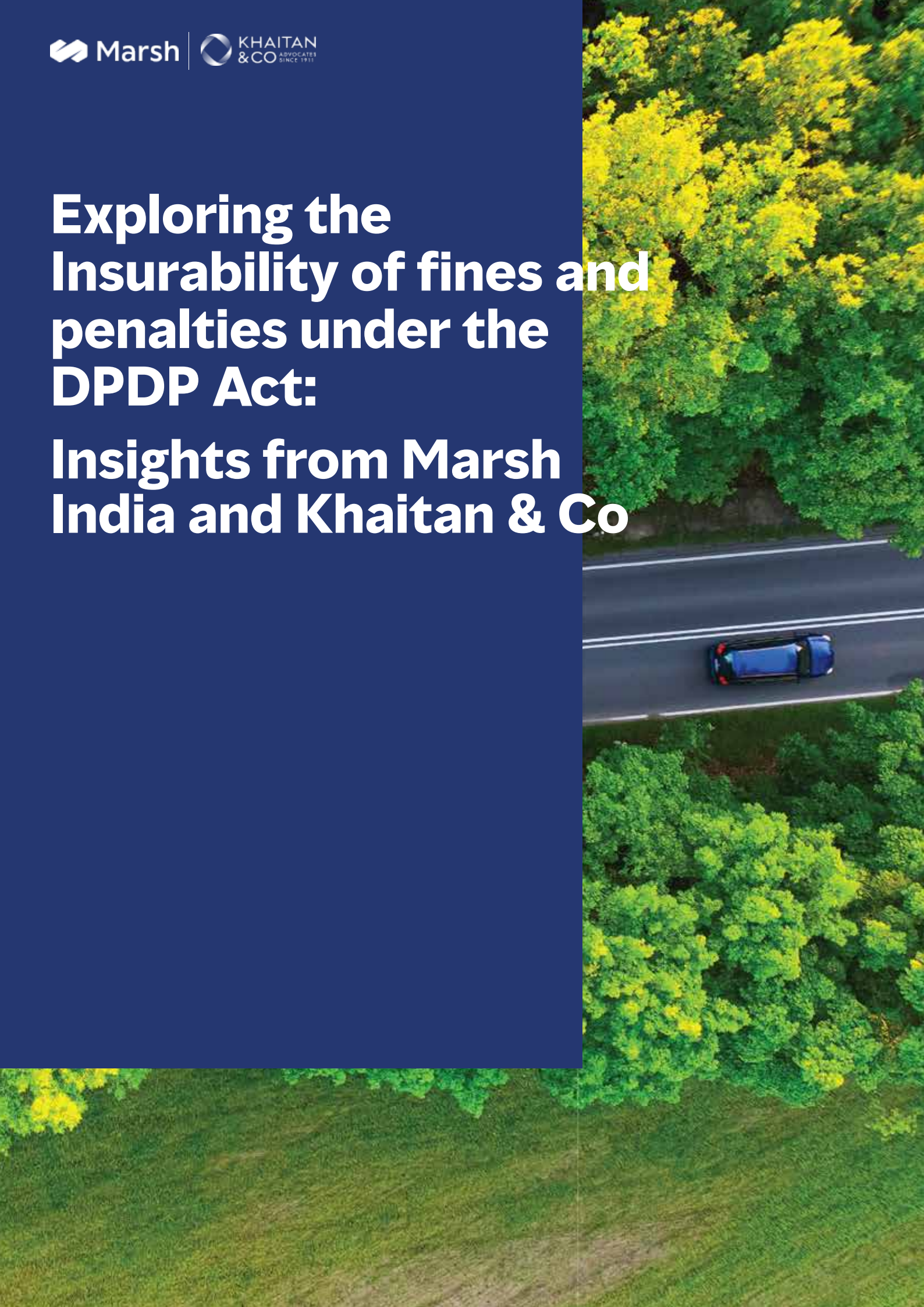
Marsh | KHAITAN &CO ADVOCATES SINCE 1911

Exploring the Insurability of fines and penalties under the DPDP Act:

Insights from Marsh India and Khaitan & Co



Introduction

The recently enacted Digital Personal Data Protection Act 2023 (“DPDP Act”) ushers in a transformative era in India’s data protection landscape. Cyber insurance policies traditionally cover losses from third-party breaches, data protection, and cybersecurity obligations. Typically, these policies cover first-party costs, such as the cost of forensic experts, data restoration, and public relations, linked to third-party actions rather than the business's fault. While these policies historically mitigated losses caused by others, the DPDP Act raises the question of whether insurance can protect against risks from non-compliance by a person with the law per se.

The Insurability of Penalties under the DPDP Act:

Under the DPDP Act, penalties may be posed for a breach of its provisions which are 'significant'. The penalties for certain individual non-compliances with certain provisions can be as high as INR 250 crore (approximately USD 30 million). Unlike global data protection laws, such as the EU General Data Protection Regulation ("**GDPR**"), which imposes a ceiling on highest penalty (i.e., 4% of the annual global turnover of the business), the DPDP Act allows composite penalties from the Data Protection Board of India ("**Board**"), for non-compliance with more than one provision.

Despite the dependency by businesses on external parties for ensuring compliance with the DPDP Act, notably, the entire responsibility for compliance is imposed on 'data fiduciaries', i.e., entities determining the 'purposes' and 'means' of processing personal data, either alone, or in conjunction with other persons. Entities processing personal data on behalf of data fiduciaries, i.e., "data processors", are not subject to any directly applicable obligations under this law. Instead, data fiduciaries are required to execute written contracts with data processors to ensure compliance.

While data fiduciaries may insulate themselves from liability attributable to data processors by contractually passing down requirements under the law to data processors, indemnity alone may not be as useful as upfront insurability of these fines. From an insurability perspective, it becomes important to examine the structure of various compliance requirements under the DPDP Act which are principles-based. For instance, the DPDP Act requires: (i) consent to be free, specific, informed, unconditional and unambiguous, (ii) personal data to be processed only until necessary to fulfil the specified purpose, (iii) data fiduciaries to implement appropriate technical and organizational measures, and (iv) reasonable security safeguards to prevent a personal data breach.

The benchmarks for compliance with these requirements may be subjective as the DPDP Act is at a nascent stage. For example, what constitutes "appropriate" technical and organizational measures may involve subjective considerations. Without clear guidance on identifying the precise benchmark of measures that are required to be implemented, entities can possibly avail of data protection or cyber insurance policies to cover any inadvertent non-compliance with the provisions of the DPDP Act, if due diligence was undertaken by the entity to begin with. The meaning or threshold of many of the requirements under the DPDP Act would possibly become clearer through judicial precedents going forward.

Other considerations:

It is commonly argued that if organisations can insure against these fines, they may have less incentive to invest in robust data protection measures. While the insurability of data protection fines raises concerns, these risks can be managed through careful policy design and implementation. Insurance providers often require policyholders to adhere to best practices and undergo regular audits, fostering a proactive approach to regulatory adherence. The insurability of penalties can create incentives for organisations to invest in compliance measures and continuous improvement, ultimately fostering a culture of accountability and adherence to legal standards.

Learning from global experience:

In the EU, courts across different member states have varying opinions on the insurability of fines under the EU General Data Protection Regulation. In some EU member states, fines that are punitive in nature have been characterized as uninsurable. In other instances, courts have considered the specific circumstances and the wording of an insurance policy to assess whether coverage may apply.

Possible scope under the DPDP Act:

There is presently a lack of clear guidance in the DPDP Act concerning the extent to which fines under the DPDP Act are insurable. That aside, it is important to note that all contractual terms are subject to the caveat, under Section 23 of the Indian Contract Act 1872 ("Contract Act"), that where the object of an agreement is contrary to public policy, such an agreement is void.

Indian courts have extensively interpreted the 'public policy' exception to the enforceability of contractual provisions as a high bar, only to be invoked in cases where there is clear and uncontestable harm to the public. Indian courts have held further that the doctrine of public policy is somewhat dynamic and fluid, and has an uncertain content, as a result, a determination of whether a contractual provision is contrary to public policy is an analysis that courts are required to make on a case-to-case basis. While Indian courts have considered the validity of provisions of insurance contracts on the touchstone of public policy, these have tended to address questions of the validity of clauses limiting the insurer's liability, restricting claim periods, or allowing for the policy to take effect after a period of time subsequent to the premium being paid, under the insurance policy in question.

There is limited judicial guidance concerning whether there are public policy restrictions under the Contract Act on what subject matter can be insured. However, Indian courts have repeatedly enforced insurance contracts covering liability for medical negligence, and for compensation due under the Motor Vehicles Act 1988, including for issues such as rash and negligent driving, and claims for statutory compensation under the Workmen's Compensation Act 1923.

Similarly, the Companies Act 2013 expressly recognizes that companies can take out professional liability insurance for their key managerial personnel, CXOs, directors,

managers, etc. in relation to any negligence, default, misfeasance, breach of duty or breach of trust in relation to the company. While there is no absolute certainty surrounding the possibility of insurance coverage of statutory fines under Indian law, in the DPDP Act context, there exists a reasonable degree of support to the insurability against the consequences of violations of fiduciary, professional, and/or statutory duties, as the same have historically been enforced by Indian courts, recognized by Indian statutes, and even mandated by Indian regulations. Cyber insurance policies in India do provide a cover for regulatory fines and penalties (where insurable by law) and by way of extension some carriers may also provide cover for "punitive and exemplary damages" as well. Notwithstanding these considerations, however, cyber insurance policy may still comprehensively cover other associated costs in relation to a cyber breach incident, including but not limited to the following:

- Costs associated with cyber incident management or crisis management;
- Notification costs;
- Credit monitoring costs;
- Public relations;
- Data restoration/recovery; and
- Defence costs in relation to any third-party disclosure liability, failure to prevent unauthorized access, failure of system security to prevent a cyber-attack, regulatory response costs, etc.

Conclusion:

While clarity on insurability of DPDP Act fines from an enforcement standpoint remains to be witnessed, insurance providers can play a vital role in managing risks and supporting businesses in their efforts to comply with data protection regulations. As the judicial stance becomes clearer, insurance policies can be tailored to address the specific needs and challenges of DPDP Act breaches, providing organisations with the necessary protection and peace of mind. By balancing the need for financial stability and compliance incentives, insurers and regulators can work together to enhance the effectiveness of data protection regulations and to safeguard personal data.

Marsh | KHAITAN & CO ADVOCATES SINCE 1911