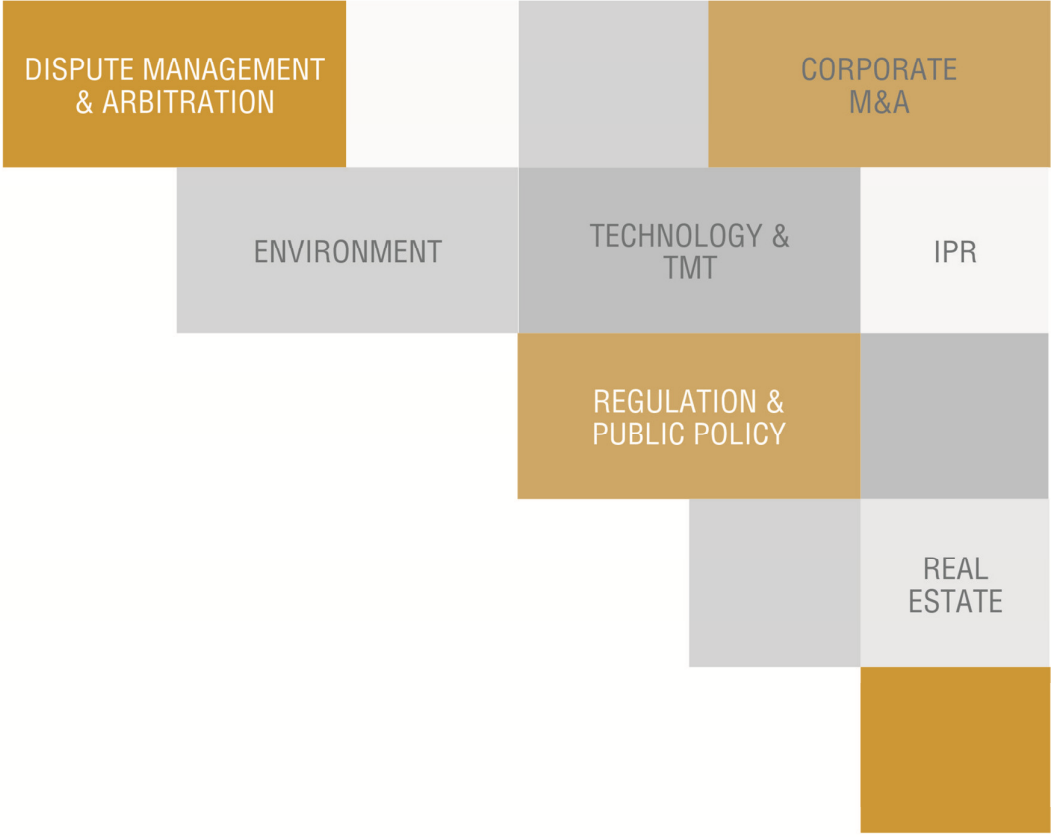

HAMMURABI
& SOLOMON
Advocates & Corporate Law Advisors

GDPR Compliance

A Challenge for Boards & Directors in India

Interestingly, the provisions of the Companies Act, 2013 have already put the onus on the Boards and Directors of Indian companies to sign off legal compliance and therefore require Indian Boards and Directors to be pro-active and drive compliance of the provisions of GDPR. The content below seeks to flag major areas where Boards and Directors need to focus in a way to best comply with best GDPR in India.

1.Data Controller/Data Protection Officer

Every Indian company should have a Data Controller/Data Protection Officer (DC/DPO) responsible for data protection in organizations engaged in the handling of individual's data. The DC/DPO should be accountable to the Board, and the Board should clearly set his/her roles and responsibilities.

2. Review of Existing Data Handling Processes

Indian companies should review their processes related to data collection, data storage, and transfer of data, including scope and ambit of consents obtained from individuals in relation to holding and use of data particularly from the perspective of such consent being unambiguous, specific, and informed. Challenges and risks thrown up following the review should be mitigated by organizations by process changes well before GDPR coming into force.

3. Data Protection Advocacy

Indian companies must implement and monitor a structured data protection advocacy program to increase awareness, impart training, and to sensitize their employees and stakeholders on the impact of GDPR on its business to achieve compliance of GDPR.

4. Continuous Mapping of Data Protection Processes

Indian companies must have transparent and verifiable mapping of data protection processes including documentation of compliance to enable regular review by an organization.

5. Conduct Checks for Data Breaches and Data Security

Indian companies need to continuously conduct checks for data breaches and data security to check the effectiveness of data security systems and processes to identify, neutralize, and report any breach well within the reporting timeframe.

6. Compliance by Third Parties

Indian companies must ensure that all third parties engaged by organizations for processing, storage, and management of data comply with GDPR. Some examples - Cloud partners, payroll management agencies, marketing partners, etc. may qualify as such entities. Requisite process should be put in place to ensure compliance of GDPR by such third parties and for review and verification by an organization.

7. Strategic Data Planning on an Ongoing Basis

Boards must ensure that Indian companies have a futuristic approach to data protection issues in the rapidly evolving regulatory regime around the globe. Therefore, continuous and ongoing strategic planning and re-calibration of strategies from time to time to meet the emerging regulatory environments and technological challenges should be at the centre of Indian Boards going forward.

8. Meet the "Right to be Forgotten" Norm

Require the company to have effective "right to be forgotten" capability, i.e., ability of a data to be effectively deleted where such a choice has been made by the individual. This would require tracking of data both online and offline and would require data management tools to be upgraded where required to be able to manage and comply with the "right to be forgotten" requirements. It is therefore essential for organizations to set up data protection frameworks at every level of their businesses and throughout the complete cycle of their processes.

Indian Boards and Directors, therefore, have to pro-actively ensure transparency and trust among all stakeholders in the data protection space in order to effectively achieve compliance with GDPR and the emerging data protection and privacy regime in India. Needless to say, Indian companies need to have internal frameworks and policies in data protection which are far deeper aligned to data protection regimes in other jurisdictions as well in order to effectively insulate the

Indian Companies against the risk of financial and non-financial exposures owing to breaches in data handling or non-compliance with data protection laws across jurisdictions. The gaps between data protection laws of different jurisdictions applicable to the same Indian company would no doubt give rise to multiple interpretation issues and compliance challenges for the company, but the framework and policies of the company will have to be capable of enabling the company to meet such challenges.