October 2019

GORNITZKY
80 Years of Excellence

From GDPR to CCPA and beyond: adopting a risk-based approach to global data protection compliance.

Managing a company's data protection compliance risks used to be simple: you could rather easily know which data protection laws applied to your company and what you needed to do to comply with them. You also knew who your regulator was and were fairly familiar with that regulator's enforcement powers and policy, as well as with the exposure emanating from data protection-related litigation in your jurisdiction. All of that has been rapidly changing in the last few years and is expected to continue to change.

Evolving data protection laws worldwide are increasing the legal exposure to companies with global operations. Companies that have invested significant resources to comply with the EU General Data Protection Regulation (GDPR) are now struggling to comply with the California Consumer Privacy Act and may, in the near future, need to revise their practices further to meet new data protection laws that are in development. Considering the changing legal framework in this field, companies should implement a coherent risk-based approach for their global data protection compliance to efficiently manage legal and regulatory risks. A lot has been written on how to comply with GDPR, CCPA and other data protection laws. This article is different. It focuses on how a company should determine “what” data protection laws to comply with and in what order, rather than on “how” to achieve compliance with a specific law.

1. Mapping. The first step in implementing a risk-based approach for data protection compliance is understanding which worldwide data protection laws apply to the company’s operations and what obligations such laws impose. Such applicability is typically determined based on the following criteria: (a) jurisdictions where the company has offices or otherwise operates through stable business arrangements; (b) jurisdictions where the company collects or processes personal data (including, *e.g.*, collection in the context of the online offering of goods or services to data subjects (whose information is processed) in the relevant jurisdiction); (c) jurisdictions where data subjects are located;

(d) the types of data subjects to which the personal data relates (many jurisdictions provide special protections to certain groups of data subjects, *e.g.*, children); (e) the types of personal data that the company processes and the purpose of processing relating to each such type; and (f) the sector in which the company operates (many jurisdictions have data protection laws that regulate specific sectors, such as healthcare, financial services, etc.).

2. Risk assessment and prioritization. Ideally, after understanding what data protection laws apply to a company's operations, the company should quickly act to implement all requirements under applicable laws. However, considering the rapidly changing legal framework in this field, and assuming that the company's data protection compliance resources are not unlimited, the company will typically need to prioritize its compliance efforts. To facilitate such a prioritization, the company must understand the potential exposure in each relevant jurisdiction. The level of exposure is determined, *inter alia*, by the possible sanctions for noncompliance, the potential for litigation, the scope of authority of local regulators and their enforcement policies.

3. Benchmarking. The next step is choosing an appropriate benchmark for compliance. The benchmark should be a data protection law that applies to the company's operations and was found to be a 'high priority' in the prioritization exercise (Step 2 above). Ideally, the benchmark would be a law that most comprehensively covers the global data protection requirements that apply to the company. Presently, a commonly used benchmark for this purpose is the GDPR, which is perhaps the world's most comprehensive data protection law and one that creates substantial exposure for incompliance.

4. Implementation. After choosing a benchmark, the company should take steps to comply with the requirements of such benchmark. This would typically entail a gap analysis, comparing the company's current level of compliance against the requirements of the relevant data protection law, as well as constructing, and executing, a plan for closing the gaps identified in the process. As part of the implementation process, the company would generally need, among others, to review its policies and procedures, document its interactions with personal data, appoint stakeholders, review relationships with third parties that have access to personal data and conduct training for personnel.

5. Comparison. Once the benchmark has been fully implemented, the company should turn back to the mapping, risk assessment and prioritization results from the beginning of the process (see Steps 1 and 2 above). It then needs to compare the requirements of each law that was considered a 'high priority' to the requirements of the benchmark. This can be achieved, for example, by consulting local data protection counsel in the relevant jurisdictions to understand what requirements under the local law are not already covered by the benchmark (*e.g.*, what steps must an online fashion retailer that is compliant with GDPR take to be compliant with the Brazilian General Data Protection Law). Once the

additional requirements are identified, the company should take steps to implement them, similar to its implementation of the benchmark requirements (as described in Step 4 above).

6. Monitoring Changes. As data protection laws are changing rapidly, companies need to monitor changes to existing laws and new potential risks related to data protection in each jurisdiction where they are active or are considering to enter. News of such changes are often provided in client updates circulated by law firms. The International Association of Data Protection Professionals (IAPP) also offers updates on changes to data protection laws worldwide. However, to be confident that any change that could impact the company is monitored, you should obtain legal advice from a data protection attorney. Companies should evaluate the risk and potential exposure from changes to data protection laws and update their prioritization (as discussed in Step 2 above) accordingly.

Compliance with the rapidly changing data protection laws is a substantial challenge for companies with global activities; and that challenge is not expected to diminish in the near future. To efficiently address the challenge, companies should change the way they think about data protection compliance: much can be achieved in a one-time data protection compliance project, but as laws and potential exposure constantly change, companies should carefully plan for a long distance run rather than a sprint. Adopting a risk-based compliance approach is important to ensure that you are running at a good pace and avoiding major hurdles.

For further information please contact:

Assaf Harel, Partner
assafh@gornitzky.com