Impact of GDPR and MENA Data Protection Laws on Company Valuations

Haroun Khwaja - Senior Counsel - Digital & Data
- Dubai International Financial Centre

“Previously seen as a secondary concern in our region, there is a new emphasis placed on privacy compliance. Companies are exposed to both legal and severe reputational risks if they do not meet their obligations.”

-Haya Al-Barqawi

Value of data v. Risk of breach

Data is fast becoming one of the most important assets for most businesses and nations. More and more companies are increasingly reliant on data in pursuing business objectives ranging from driving internal automation and digital transformation to improving algorithms used in customer facing applications. Data is frequently hailed as the new oil, with companies and even some governments seeking to claim ownership to it (despite it arguably being a personal asset which belongs to the individual to whom the data relates). However, what sometimes seems to be missed is that data, much like oil (to take the analogy of oil spills), is a double edged sword; whilst it promises to be a key driver of innovation and new source of wealth, if handled without care, it can also turn out to be the cause of significant financial and reputational damage to the guardians and beneficiaries of such data (particularly in the case of personal data). Take for example, the data scandal that engulfed Facebook and Cambridge Analytica (a British political consulting firm). Facebook’s market capital valuation dropped by USD 35 billion and customer mistrust took hold, shortly after news of the data breach broke out. Cambridge Analytica had, without consent, harvested and used the personal data of approximately 50 million Facebook profiles for political advertising purposes. Only a few months later, CNBC reported that Facebook posted another USD 120 billion drop in its market valuation after missing analysts’ projections on key valuation metrics such as revenue and advertising figures (which one may reasonably speculate to have been attributable to the Cambridge Analytica incident), and shortly thereafter Facebook lost roughly 3 million daily users in the EU following the introduction of the General Data Protection Regulation (‘GDPR’).

GDPR’s limited impact on MENA entities

In the last year or so, more and more companies in the MENA region began to take notice of data protection compliance largely due to the extraterritorial application of the GDPR and the associated hefty penalties it imposes for non-compliance. The penalties under the GDPR range up to EUR 20 million or four per cent (whichever is higher) of an entity’s total worldwide annual turnover in respect of the previous financial year. Up until more recently, data protection compliance was largely a concern for MENA based companies that offered goods or services to, or monitored the behaviour of, persons in the EU (particularly start-ups, e-commerce platforms and other tech enabled companies that handle large volumes of personal data in the course of their business).

Proliferation of regional data protection laws – a complex compliance challenge for all

With the surge in local data protection laws in the region, with some already in place and others revised to align more closely with the GDPR (for example the UAE's Dubai International Financial Centre (DIFC), Lebanon, Morocco, Qatar and Tunisia), newly enacted ones (for example Bahrain and Egypt) and others expected to be introduced in the near future (for example the UAE (onshore) and KSA), data protection compliance has become crucial for all entities processing personal data in the region (and no longer only those providing goods or services to, or monitoring the behaviour of, individuals in the EU).

As such, there is an increasingly complex data protection landscape, both across and within jurisdictions in the region, that entities will need to navigate. For instance, although the UAE does not currently have a comprehensive modern data protection law, it does have provisions relating to privacy in a number of federal laws. Examples include the Penal Code, the Telecommunications Law and the Anti-Cyber Crime Law (which all carry criminal penalties), sector specific data protection provisions (such as the Dubai HealthCare City Authority's regulations on the retention, use, disclosure and transfer of patient health data) as well as data protection laws that are specific to the financial free zones (namely, the Dubai International Financial Centre and the Abu Dhabi Global Market). It remains to be seen if the anticipated UAE federal data protection law (if and when enacted) will override the existing privacy related laws, and if not, how it will interact with them. In particular, it will be interesting to see whether personal data can be transferred between the mainland and the various free zones.

Obligation to comply with multiple federal laws

Although most of the national data protection regimes share, to some degree, similar concepts and principles (such as the lawful bases available for the processing of personal data, restrictions on transfer of personal data abroad, breach notification requirements etc.), significant differences exist. An example would be the differing timeframes under the various national laws within which individuals and the relevant regulator are to be notified in the event of a personal data breach. If a company or organisation with operations in multiple countries were to suffer a personal data breach, it would have to notify the regulator and the affected data subjects in the relevant jurisdictions in accordance with the breach notification requirements (if any) in each of those jurisdictions. To illustrate this further, an Egyptian company with operations in both Egypt and Qatar, would have to comply with both the Egyptian Data Protection Law and the Qatari Data Protection Law (in respect of personal data of individuals in Qatar). So, if a data breach were to occur affecting individuals in both countries, the company would need to notify the Egyptian Personal Data Protection Centre within 72 hours from the time of the breach, and data subjects to be notified within 3 days (from the time the Personal Data Protection Centre is notified). Additionally, the company would need to notify the Qatar data protection authority, however given no such timeframe is specified, it would be reasonable to expect that such notification should be made without undue delay.

It is important to note that an entity's compliance with its obligations under the laws of one jurisdiction, will not excuse it from having to comply with the laws of another jurisdiction that also applies to it (for example by virtue of the company's processing of personal data relating to that country as well). That is, an entity's obligations to comply with more than one federal law in such a scenario, exists in parallel, and is not mutually exclusive. Consequently, companies with international operations, will need to ensure their regional or global compliance programme is tailored to manage their compliance obligations with each of the national laws having regard to the legislative disparities and local nuances. Having said that, the majority of these regional laws have been drafted with the GDPR (or its predecessor EU Directive in mind). As such, entities that are already GDPR compliant have a solid foundation, and need only adjust their

compliance activities in each jurisdiction to account for the obligations that are different to, or more onerous than the GDPR.

Increasing focus at board level

For the reasons noted above, there has been increasing focus at a board level in the EU, Australia, Brazil, Canada, Japan and certain States in the US (most notably California) on both internal compliance and the compliance status of potential target companies in a corporate transaction context. Consequently, some deals have been failing to close around the globe because of concerns in relation to the target's data protection compliance. This trend is likely to be more pronounced in the MENA region in this new era of proliferating modern data protection regimes.

It is also likely that data protection compliance will begin to receive heightened attention by the boards and management of entities throughout the region due to the fact that some of the regional data protection laws, for example the Bahrain Personal Data Protection Law and the Egyptian Data Protection Law, impose criminal penalties (in the form of imprisonment and/or fines) for breaches of various provisions that would typically be the subject of civil penalties under other modern data protection regimes. This raises the stakes for board members and management of entities in the MENA region.

Impact of compliance on profits and valuations

As is the case under the GDPR, regional data protection laws impose penalties (in some cases of a criminal nature as noted above) for non-compliance, and both listed and privately held companies face the possibility of reduced valuations (if potential acquirers were to determine, during the course of their due diligence activities, that the relevant target is not compliant with the data protection laws of one or more jurisdictions in which it operates, but the acquirer nevertheless elects to proceed with the deal).

If in such a case, the target cannot demonstrate (by way of its documentation, policies and technical and organisational measures) that it has been, is, and will be compliant going forward with its data protection obligations, the acquirer should seek a reduction in the purchase price and/or seek revisions to the share purchase agreement (for example by including appropriate indemnities to protect it against any potential financial penalties that may be imposed by regulator(s) and compensation claims that may be brought by individuals affected by a previous breach). Further, it is recommended that an additional 'buffer' be embedded into any price reduction so as to offset any costs that may also be incurred (separate to regulatory fines) post acquisition in remediating the operations of the target (for example the need to undertake more detailed assessments, implement appropriate technical and organisational measures, hire new resources such as a Data Protection Officer, and roll-out training across the organisation etc).

As noted above, given that some jurisdictions in the region impose criminal penalties for certain breaches, price reductions and indemnities will not provide adequate protection, which ultimately may result in deals that are not closed for fear that management and officers of the acquiring company may be held to account, although one would expect that authorities would be unlikely to sanction the new management for the violations of the previous administration.