M&A transactions involving data-intensive target companies: a check list

Omar S Bassiouny and Suzanne El Akabaoui of Matouk Bassiouny & Hennawy discuss how share purchase agreements can be adapted to suit M&A deals involving companies where data is the main asset

www.matoukbassiouny.com

In recent years and in accordance with the sustainable development strategy for 2030, Egypt has taken significant steps to create a legal environment capable of fostering the development of the online sphere and regulating internet activities.

More specifically, Egypt has seen rapid legislative developments and a wave of reform in the areas of cyberspace, information technology and the regulation of internet activities. The newly enacted laws aim to regulate online activities, safeguard content and data available online, eliminate cybercrimes and provide protection for online users.

Digitisation has increased the amount of data generated by and about individuals, rendering data a commodity, an asset and an input for goods and services. In fact, businesses are deriving value from the data collected during the course of their activity by analysing it to improve the quality of the products or services, to develop new products, to predict usage patterns and to target sales through targeted online advertising.

In light of the increasing importance of data as a commodity worldwide, Egypt started developing a legal framework defining and regulating the concepts and elements forming the digital markets spaces, fintech activities in banking and non-banking financial services, and generally working on creating a legal infrastructure protecting data generating subjects to ensure that their fundamental rights are overseen and that the economic value of data is preserved.

In this context, the Egyptian Private Data Protection Law No. 151 of 2020 (PDPL), which draws upon the General Data Protection Regulations (GDPR), was enacted. It focuses on safeguarding the personal data of individuals, which is collected, stored, processed and transferred cross border electronically through online platforms. Also, the definition section in the PDPL introduces new concepts

Omar S Bassiouny
Founding partner and head of corporate and M&A, Matouk Bassiouny
T: +202 2796 2042 (ext.191)
E: omar.bassiouny@matoukbassiouny.com

Omar S Bassiouny is a founding partner of Matouk Bassiouny and head of the corporate and M&A group. He is consistently ranked in the top tiers and bands by legal periodicals in the areas of corporate law and mergers and acquisitions, reflecting his considerable expertise in setting up joint ventures and new projects in Egypt ensuring compliance with local laws and corporate governance.

Omar is also recognized for his negotiation skills and business sense. Omar focuses on all corporate matters including M&A, public takeovers, restructuring and cross-border transactions. In addition to corporate issues, Omar has significant experience of all aspects of investing and doing business in Egypt.

Suzanne El Akabaoui
Of Counsel, Matouk Bassiouny & Hennawy
T: +202 2796 2042 (ext. 362)
E: suzanne.elakabaoui@matoukbassiouny.com

Suzanne El Akabaoui is a multicultural attorney at law, holding degrees in law from the University of Paris, Sorbonne and economics from Cairo University. She has nearly 20 years of professional practical and consulting experience, having advised a wide variety of local and international businesses and NGOs.

Suzanne's practice focuses on data privacy, ICT and media, general corporate, intellectual property rights, trademark and patent registrations, business and investment-related consultations covering banking, corporate and commercial law, as well as civil labour and commercial litigation.

relevant to cyberspace and sets the legal infrastructure necessary to guarantee its proper implementation.

The yet-to-be-established Private Data Protection Centre (PDPC) should act as the regulatory authority for the protection of private data.

Summary of the law

The PDPL allocates rights to 'data subjects' (any natural person to whom electronically processed personal data is attributed that identifies them legally or factually and enables their identification from any other person).

Meanwhile, it imposes obligations on 'controllers' and 'processors'. Controllers include any natural or juristic person who has, by virtue of the nature of their activities, the right to obtain personal data and to specify the method and criteria of retaining, processing or controlling such data according to a specific purpose or to their activities. Processors are defined as any natural or juristic person competent, by virtue of the nature of their work, to process personal data for their benefit or for the benefit of the controller by way of an agreement with the controller and in accordance with his instructions.

The PDPL has extraterritorial jurisdiction and its provisions apply to any person violating it if the offender is an Egyptian national residing in Egypt, a foreigner residing in Egypt or a foreigner residing abroad provided that the violating act is punishable in any form in the country where it occurred and the data subject of the crime belongs to Egyptians or foreigners residing within the Arab Republic of Egypt.

As is the case for most data privacy laws and regulations in the Middle East, protection of the data subject in Egypt is granted through the stringent requirement to inform data subjects about the processing of their data and obtain their clear express consent prior to storing, controlling, processing or transferring cross border the said data.

Obligations of data controllers and data processors under the PDPL revolve around obtaining the data subjects' consent on the use of their data, putting in place strong technical cybersecurity measures and solutions, doing security impact assessments and entering into detailed and tight agreements with controllers and/or processors (controller-to-controller agreements, controller-to-processor agreements, data sharing agreements, data transferring agreements, SCCs, SaaS and TaaS solutions agreements, etc.).

The criminal liability of the data protection officer, the *de facto* manager and/or the corporate entity itself triggered by the noncompliance with the provisions of the PDPL requires the corporate entity to act diligently in establishing that it has exerted its best effort to comply with the legal, regulatory and technical requirements under the PDPL.

What to look for in an M&A transaction

Given the nature of data-intensive businesses, where data is considered as the key asset, considerations in M&A transactions due diligence processes must expand to review additional areas. In Egypt the regulatory authority has not yet been established. The market must wait for the issuance of the PDPL Executive Regulations to compile an exhaustive list of the matters that need to be reviewed during a due diligence process.

However, a reading of the law and a review of international practices allows the compilation of a non-exhaustive list of the potential matters that need to be addressed during the due diligence process for a data-intensive target company (target).

1. Data-intensive companies

Data-intensive companies (DICs) are businesses whose activity is based essentially on the collection and analysing of their customers and users' personal data and information.

Many of today's industries have become

"Egypt has seen a wave of reform in the areas of cyberspace and information technology"

increasingly defined by big data and analytics. Sectors that have seen the most development in such areas are medicine, retail, construction, banking, and transportation. M&A transactions in these sectors are likely to require a more diligent data protection health check exercise on the target to avoid the criminal sanctions associated with the breach of the PDPL legal provisions, regulatory requirements, technical and security checklists.

2. Acquirer's checklist

The PDPL requires that holders, controllers and processors of data obtain data subject consent for the storage, collection and processing (when applicable) of the data. Ultimately, in the due diligence process, the acquirer must get comfort that the target has obtained data subject consent on the disclosure of the data, in addition to the rights of storage, collection, processing and, where applicable, the cross-border transfer of the data. Further, in cases where the data subject's data is used for electronic marketing, the acquirer must check that the consent is granted for the purpose of receiving electronic marketing.

Given that controllers and processors are subject to license and permit requirements under the PDPL, acquirers must review the validity of those licenses and permits depending on the legal status of the target as controller, processor or both. The target's data protection officer must be involved in the due diligence process, prepare the required documents for acquirer's review and be equipped to answer any questions raised in relation to permits granted by data subjects to use of their data for secondary purposes (if applicable).

A thorough review of the target's privacy policy should be undertaken in cases where the target has a direct relationship with consumers. This review will entail the review of the consent forms, whether the collected information was used strictly for the purpose described under the privacy policy, applicable laws, and the agreements between the consumer and the target company. The acquirer should also review whether opt-out or deletion of data requests by data subjects were duly honoured.

In the case of processors collecting data from a business in the course of providing services to such businesses, acquirers should check whether such data collection was done within the limits of the agreement between the processor and such customers (controller-to-processor agreements).

Restrictions on disclosure to third parties could limit the transferability of the data. In such cases, it is important that acquirers review any terms relating to the ownership of aggregated or anonymised data. If the target's customer retains ownership and use of data under a license agreement, it is very probable that the license agreement includes a limitation to the assignment or transfer of the underlying agreement. Acquirers must clear such restrictions with the concerned party.

In assessing the target's position with respect to legal actions filed against it, acquirers should seek information on whether legal action was taken against the company for violations of privacy laws or cybersecurity laws. When the regulatory authority is established, acquirers must seek its confirmation that the target was not subject to any data breach and that no legal action was filed for a data breach.

Generally, the acquirer must diligently review the target's consumer-facing privacy policy (where applicable), data collection, storage, use and security and all relevant contracts.

In the case of DIC acquisitions, it would be safe for the acquirer to operate an information technology security due diligence check. IT specialists should be part of the legal due diligence team to confirm whether or not the technical security requirements provided for under the PDPL and Cybersecurity Law and the contemplated regulatory authority regulations are duly met by the target.

"Data-intensive business acquisitions are expected to rise in the near future"

3. Share purchase agreement clauses

Suggested matters to be addressed in the share purchase agreement (SPA) for an acquisition of data-intensive targets:

- Definitions section

Clearly define the nature of the data to be disclosed (define the category of the data under which the data collected by the target comes under the PDPL, for example sensitive data, children's data, individuals medical histories etc.).

Also define which laws apply to the type of data subject of the agreement and the relevant obligations and tools to protect such data. Ideally language used in the standard contractual clauses and definitions under the PDPL and GDPR should be used.

- Allocation of data transfer risks

Parties must agree on the allocation of risks for improper transfer or disclosure of the data.

- Reps and Warranties

The seller will represent and warrant that:

  - It has the right to transfer the rights to any data owned thereby or licensed thereto under either the law or agreements with the seller's data providers;
  - The seller is compliant with the applicable data privacy laws and its own privacy policies;
  - The seller (if applicable) has not been subject to any legal actions taken against it alleging the violation of data privacy laws or has not been subject to any data breaches;
  - The seller has put in place a strong and solid security system to guarantee that data collected thereby is properly protected.

- Indemnities section

The selling party should indemnify the acquirer for claims relating to: data breaches; penalties inflicted by the regulatory authority for violation of applicable laws and regulations; and the failure to establish or obtain the right to sell, license or transfer any data subject of the sale transaction.

4. Risks contemplated under competition laws

In the context of a free market, safeguarding competition requires the restraint of anti-competitive behaviour essentially by limiting the abuse of the consumer by a dominant market player.

Digital markets are intrinsically more competitive markets. They differ from the traditional markets in that they are characterized by heavy innovations, which tend to create winner-takes-all dynamics. Additionally, digital markets have low barriers to entry due to low fixed costs, lower switching costs, direct and indirect network effects, multi-homing, and global effects and customer segmentation. All of these could ultimately lead to customer and price differentiation and discrimination practices.

Based on these issues, we may expect a shift in the norms on which merger assessments are made by the Egyptian Competition Authority (ECA). The digital market characteristics may lead the ECA to develop new norms to identify the magnitude of the impact of data shared in a merger on competition, consumer welfare and consumer data privacy rights.

A review of the international practice in assessing mergers by various competition authorities suggests that the ECA may develop new merger assessment tools as follows:

1. Introducing new assessment tools

Assessing dominance is one of the competition authorities' key roles when carrying out a merger assessment. While in traditional markets dominance can be easily established through economic measurements, the nature of mergers in the digital markets means these economic tools are unreflective of the actual impact of a merger in a digital market on the consumer welfare. The interchangeability and substitutability of products is no longer sufficient to define markets.

Similarly, applying dominance indicators such as market share of the dominant undertaker and constraints to entry or expansion in the market is no longer effective or indicative.

Based on the above, mergers and acquisitions lawyers may be faced by rejection decisions based on new assessment tools in data-intensive M&A transactions.

2. Adapting existing tools: a more holistic approach

Alternatively, the ECA could take a holistic approach, adapting the existing economic tools to define markets, establish dominance and measure the level of impact on consumer welfare. Typically, it could identify potential threats to competition in a given market where the acquirer could leverage its dominant position and could push other market players by making the target visible in its business.

There is a risk that competition on privacy protection could be harmed where that privacy is a significant parameter on which service providers compete. Data privacy protection is currently recognized – in the international arena – as a parameter on which companies compete.

Final thoughts

While data-intensive business acquisitions are expected to rise in the near future, the practical implementation of the data privacy laws and regulations, the intrinsic nature of the digital markets and the risks associated with data usage and ownership will add another layer of complexity to due diligence processes in M&A transactions.

A proper adaptation of the SPA to the nature of data-intensive target companies where data is deemed as the main asset can mitigate the risks associated with the abstract nature of the asset.