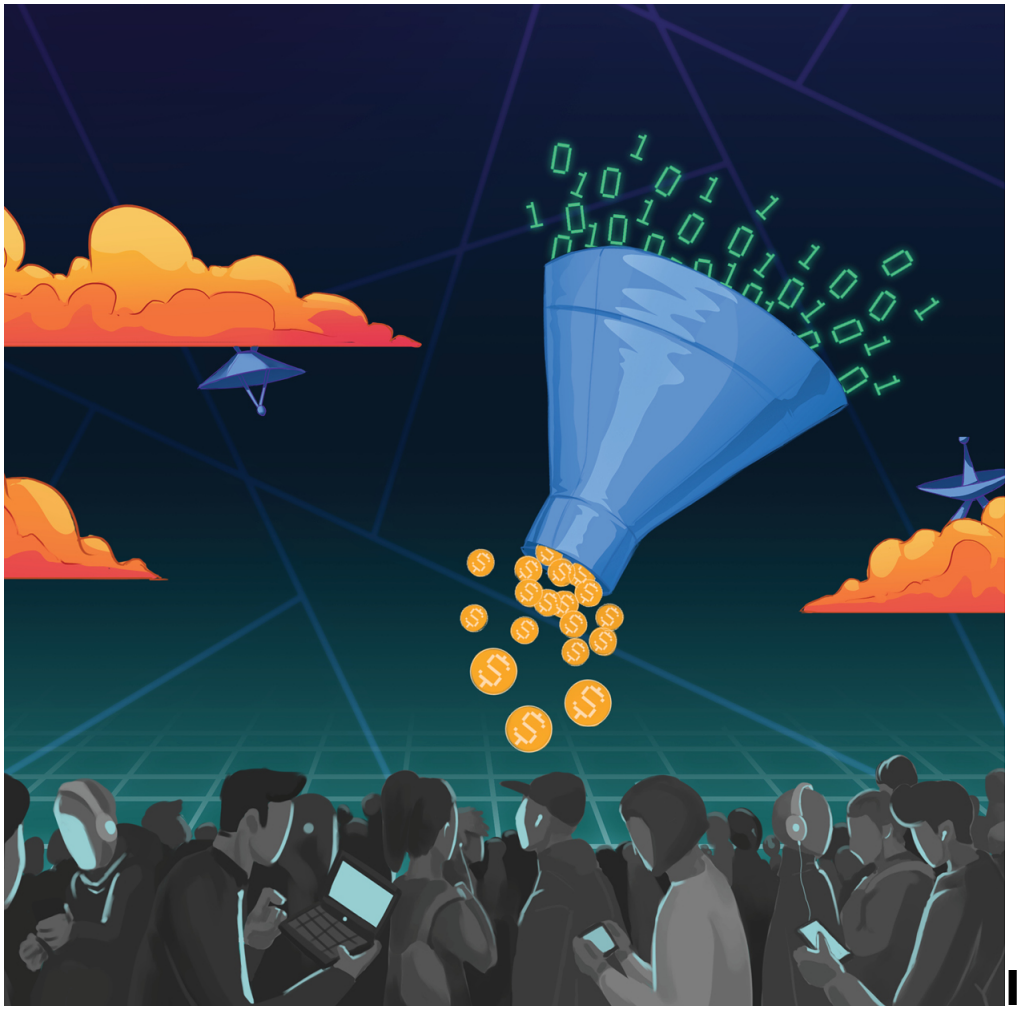
Unlocking the value in data: successfully implementing compliant data monetisation strategies

Martin Hayward - Head of Digital & Data - Digital & Data - Dubai International Financial Centre

Private: Stephen Jiew - Senior Associate - Intellectual Property - Dubai International Financial Centre



Introduction

More and more, the question from our clients is: ‘How do I make money from my data?’ Organisations are increasingly data-heavy businesses and as they seek to grow and explore new revenue streams or even new business models, they are exploring ways in which they can realise new and greater value in their data. In the world of Big Data, data has become both a key asset and a strategic differentiator.

In this article, we explore the ways in which organisations are looking to generate this value whilst ensuring they stay compliant with an ever-changing and increasingly complex web of Middle East data protection laws and continue to protect the intellectual property rights in their data.

In particular, data has become very relevant to many people in Middle East organisations who have not, traditionally, handled or been involved in data. With that comes both opportunity and risk. Whilst bundling value added data services with existing solutions may make complete sense from a sales point of view, it may, though, raise legal and regulatory challenges that need to be carefully thought through and a robust, and compliant, strategy built to ensure effective data monetisation.

What is going on with the data inside organisations?

As Middle East businesses go through a rapid process of digital transformation, they are increasingly looking for insight and advantage from the large datasets they hold and have access to in order to improve and change the way they work internally. A great deal of value is being realised internally as organisations put their data to use to drive efficiencies, reduce costs, improve quality and strengthen customer experiences.

As organisations share data across the organisation; often moving it between business units in different countries and centralising (or regionalising) the storage of data, for example. they need to ensure that they have the necessary legal rights and permissions in place (whether express or implied consent, or otherwise) under applicable laws and regulations based on the type of data they are moving and where they are moving it to. With the increasing use of emerging technologies within organisations, there is greater data mobility. An example of this is moving datasets to be mined by AI programmes for new business insights. Just because that data is moving through an organisation's internal network does not mean that it is not an international transfer that could, potentially, be subject to data protection laws and regulations.

Key to any data monetisation exercise is understanding what data you are seeking to use and share. Is it machine data from a manufacturing facility or personal data from a customer relationship management system or an employee database? If it is personal data, what types of data are involved? Personal data covering biometrics or health information, perhaps? Mapping what data it is and where it goes to is an essential, starting point for any risk analysis. Only once that risk analysis has been done can organisations consider rolling out internal data monetisation strategies and exploring external data monetisation opportunities.

What happens when the data leaves the organisation?

Data monetisation comes in many different forms. It can come directly through revenues earned from selling or licensing data to third parties (such as credit bureaus or data exchanges). Sometimes that can be exchanging data for data to enable organisations to access new and valuable data. It can come from additional revenues earned by bundling data with other products and services and selling on to customers. Increasingly, it comes from vendors offering discounts or premiums in exchange for access to key customer data. There is increasing demand from third parties for data, and increasing interest within organisations to share data with third parties for data analytics but releasing any data externally needs to be carefully considered and organisations need to review what data is being released, whether it can legally be released (in addition to whether it is, commercially, a good idea), where it is going, to whom and for what purpose(s).

Once again, the first question organisations need to ask is a simple one: 'Do I have all the necessary rights to share the data?' As noted above, this requires a comprehensive understanding of the data in question (and what that data comprises). Depending on the data, organisations need to understand whether they have the necessary legal rights and permissions in place specifically allowing the planned data sharing. Do they need to aggregate and anonymise the data? If so, can they technically do it and if so, and if they do, will this meet the requirements of applicable laws. For example, will this remove the need for consent to share the data? One challenge of data aggregation and anonymisation is the fact that the more a dataset is aggregated and anonymised, the more value it may lose.

Once the organisation has determined that it has the necessary legal rights and permissions to share the data, it needs to confirm if it can transfer that data internationally. Middle East data localisation or residency restrictions are increasing; focusing on particular types of data and particular industries. Organisations need to understand the type of data that could be affected by these localisation restrictions and where they can (and cannot) send the data. Organisations need to investigate what steps they need to take to ensure they can take advantage of the data monetisation opportunities available through international data transfers.

If data is being sent to a third party, organisations need to ensure that they have the right contract terms in place with that third party before they share the data. This is important to meet legal obligations and to mitigate risk. Contracts need to include detailed data protection, data security and IT security provisions.

They need to cover what the third parties are allowed to do with the data, who they can share it with (and on what terms), and how the data owner can get the data back (or deleted).

A critical area to cover is the organisation's IP rights in the data as the value in data, and particularly large datasets (otherwise known as 'Big Data'), is increasingly identified by organisations. Organisations will normally license rather than pass ownership in their data, usually on a non-exclusive basis, to ensure they can maximise the use and value in that data. They avoid licensing on an exclusive basis as it would result in the rights holder giving up their rights to use the IP more widely in exchange for compensation. At a time when data is increasingly valuable, rights' holders want to have control over their works. Before they can do that, organisations need to ensure that they own all necessary rights in such data. The three probable IP categories that data can be protected under are: patents; copyrights; and trade secrets/confidential information. When patenting data, it is the algorithms that are mainly able to be protected. For copyright, individual data or collection of data (databases) can be protected if they meet the requirements. With regards to trade secret protection, it is that of confidentiality of a large, undisclosed compilation of data. Access to data can be controlled. Allowing controlled access to a third party in conformance to a licence increases the value of the data and contract law can provide a legal basis for the data rights' holder to seek rewards for its investment and control over the data. The issue with that is competitors or unauthorised third parties, that are not part of the licence agreement, may try free-riding, therefore despite licence agreements helping the rights' holder control their rights in and the access to data, trade secret protection should also be considered to ensure further rights over data. To allow a party to use your IP protection under trade secrets would be with the use of some form of confidentiality or non-disclosure agreement that allows the reuse of the IP while preserving the trade secret. In regard to patent and copyright protected data, it is through the granting of a non-exclusive licence or via a public statement to a certain group of people allowing the use of the patent. Of course, the issue with not being able to more freely exchange data or have wider access to it is that it leads to less innovation. However, everyone wants to protect their data especially in an age where Big Data and artificial intelligence are becoming more popular despite the challenges they face under IP law. It seems that Big Data will most likely drive changes in our current IP laws which are increasingly seen as inadequate for protecting the vast amounts of data available.

Some organisations are not looking to directly monetise their data but make their datasets available as open datasets for developers to work on, free of charge, gaining benefit and value from the work those developers do and the innovations they generate from the datasets. Open data programmes are becoming a more common sight, particularly for government entities. The more data that is combined, the more benefit and value that can be extracted. For that reason, we see organisations teaming up to share and pool data and make it available. The contract terms governing these open data arrangements need to be carefully considered to ensure that developers can gain the full access to and use of the open datasets whilst the organisations making the datasets available can take full advantage of the work the developers do and meet their legal and regulatory obligations in relation to the data they are sharing.

Lastly, data monetisation is a particular challenge for SMEs and start-ups. For many of these organisations, data sharing could prove a key differentiator, and accelerator, in their growth but there is a lack of data awareness, or data maturity, amongst smaller (and early stage) companies. Many may also underestimate the opportunities data sharing and data monetisation offer.

With the growing trend for Middle East countries adopting European data protection legal principles which focus on regulating a previously under-regulated data economy and providing rights to individual data subjects to better control the use of their data, Middle East organisations need to ensure that their data monetisation strategies are in place, tested and future-proofed to ensure that they can continue to secure value from the data they hold.

For further information, please contact Martin Hayward (m.hayward@tamimi.com).