LEGAL BUSINESS

DISPUTES YEARBOOK 2023

BENCH STRENGTH REVISITED

In association with

STEWARTS

Navigating cross-border data flow issues in the UAE

Alsuwaidi & Company discusses issues of personal data privacy as regulated by the Abu Dhabi Global Market (ADGM), particularly from a cross-border transfer perspective

The value of data

Worldwide, the intrinsic value of data is universally accepted, and its scale and value are on the increase: in 2017 the digitally transformed world was generating 2.5 quintillion bytes of data daily, digital technology in international trade was valued between US$800 and $1,500bn in 2019, and global spending on AI is forecast to accelerate from $50.1bn to $220bn in 2024.

The recent fine imposed on Amazon for $888m is a very sobering example of the financial cost of a data breach. However, the cost is not just limited to a fine. Other adverse considerations include damage to reputation and loss of consumer confidence. Marriot's acquisition of Starwood in 2018 illustrates this point. Unbeknown to Marriot, Starwood had already been hacked resulting in the personal data of millions of customers being compromised. The United Kingdom (UK) privacy watch dog fined the hotel chain £18.4m. Had this issue been known prior to the merger, through the due diligence of data privacy issues, the whole deal could have been compromised once the magnitude of the breach was discovered because reports are that the breach had taken place as far back as 2014 and affected over 300 million customers. In 2018 Marriot had spent $28m because of the breach and is facing multiple actions for damages from aggrieved customers.

> The unwitting sharing of data with cyber criminals is an unquantifiable loss but is certainly relevant in an age where the smallest competitive advantage converts to massive gains.

Whilst we only hear of the largest data breaches and most significant fines, these are alarm bells that start-ups and small companies in the ADGM cannot ignore. Firstly, because the ADGM data privacy regime makes it obligatory to protect personal data. Secondly, consumers are alive to these issues, and a failure to adequately deal with data protection will result in a loss of confidence. Thirdly, a failure to apply data privacy safety measures is an invitation to hackers. The unwitting sharing of data with cyber criminals is an unquantifiable loss but is certainly relevant in an age where the smallest competitive advantage converts to massive gains.

Cross-border transfer under the ADGM regulations

In 2021, the ADGM introduced its second version of its data protection regulations (regulations), and as with many other jurisdictions, they are closely based on the European Union's General Data Protection Regulation (GDPR). Under part VI, the regulations establish an Office of Data Protection headed by a Commissioner of Data Protection who has a wide range of functions and powers to monitor and enforce compliance.

The coordination and regulation of cross-border transfer is by its nature a veritable minefield of uncertainty. It requires not only for different jurisdictions to be in sync with one another, but also their combined anticipation of the future impact of legislative and innovation changes.

The importance of cross-border transfers of data is recognised by the ADGM in its affiliation with the Global Privacy Enforcement Network (GPEN), an international organisation promoting the cooperation in cross-border enforcement of laws protecting privacy. On its website, the ADGM maintains a published list of jurisdictions it deems to have adequate data privacy and protection measures.

Under part V of the regulations there is a general prohibition on cross-border transfer unless certain preconditions are met. This general prohibition should be considered alongside article 3 which makes it clear that the regulations also apply to ADGM entities processing data outside its jurisdiction. An obvious example are entities who outsource telemarketing. For example, Etisalat have recently established a Do Not Call Registry governing and protecting individuals from unsolicited or malicious calls. ADGM entities utilising telemarketers in, for example the UK, calling a data subject with an Etisalat will be required to adhere to the Do Not Call Registry and will be in breach of the regulations if they do not. From a co-operation and enforcement perspective, the ADGM would in terms of article 46 of the regulations no doubt encourage and develop its international co-operation mechanisms with the UK to

give effect to any transgression of the Do Not Call List, whether it took place within the ADGM or in the UK.

The regulations, under part VII, provide the Commissioner with authority to actively monitor compliance and secondly to sanction entities found wanting in compliance with the regulations, ranging from simply ordering the production of required information reasonably required to conduct its duties to a fine of up to $28m. These administrative decisions, if disputed can be scrutinised by the ADGM Court. At the time of writing this article the ADGM has not published any fines nor are there any cases concerning the administrative decisions of the Commissioner.

Cross-border transfer: the future

With the monetising of artificial intelligence (AI) gaining traction (Open AI Generative Pre-trained Transformer (ChatGPT) assisted in the drafting of this article), we can expect more changes to data privacy law regimes. Currently the most comprehensive on the issue of AI are the GDPR and the California Consumer Privacy Act (according to ChatGPT), but there are already questions arising that require attention.

For example, according to article 4(1)(b) and (c) of the regulations, personal data must be collected for a specific purpose and cannot be used for a purpose other than originally intended (this is in line with article 5 of the GDPR). This means that data cannot be collected for an unspecified reason on the gamble of its future potential. It also means that once the data is used for its specified purpose it cannot be used for another purpose. Under article 15(1)(a) of the regulations a data controller is obliged to erase the personal data once it is no longer necessary for its intended purpose.

The opinion of this author is that this is probably too regimental because it prohibits the collection of data before its benefit is understood, which is the antithesis of AI. Additionally, once the data is collected it can only be used for its original intended purpose, requiring a data controller to again ensure compliance before using the same data for another purpose. This will increase costs and delay the potential benefit of its new purpose, resulting in an unnecessary restriction of innovation.

Another example is the requirement for the human review of significant decisions made by automated decision making, which is a principle based on article 23 of the GDPA and found in the regulations at article 20. This is a significant barrier to innovation. This restriction may be linked to a distrust of automation in the field of personal data, which may or may not be justified, but could be balanced out by the simple understanding that the consequences of any error in the automated process lies at the feet of the data controller and processor.

The real value of data is found in its transformation into information and then to knowledge. Data becomes even more valuable when combined with other information. The regulations define this as 'pseudonymisation' which is comprehensively covered in the regulations.

What is less clear is a distinction between 'automated process', the use of technology to perform tasks that would otherwise


Craig Cothill

be done manually and 'artificial intelligence' being the use of algorithms and machine learning. The regulations do not define either of these concepts. Perhaps this is so because the distinction is obvious but referring to AI as an automated decision maker has the ring of referring a calculator to an abacus.

In defence of the regulations, there is the argument that the definition of 'processing' is wide enough to cover AI, and it would be absurd to consider this definition to exclude AI. Article 30 is also relevant to the yet unknown changes that AI will bring. In the context of security of processing, it refers to the 'State Of The Art', which is a term also used in many patent laws. As defined in the regulations it means the 'current state of technological development'. This together with the wide definition afforded to 'processing' could include a reference to AI.

Intellectual property issues aside, data used by one does not prevent its use by another. In this way, data is a unique asset to be exploited by multiple parties at the same time for the same or for varying reasons. It is non-rivalrous. Thus, the benefit of data to a particular controller or processor could be useless tomorrow, but may (through, for example the use of AI) have value the next day, but for a different reason. Currently, this potential advantage must be balanced with the obligation to erase data once it has served its purpose.

It remains to be seen how the ADGM will continue to strike a balance to protect privacy and at the same time not restrict innovation.

CRAIG COTHILL
Senior associate
E: c.cothill@alsuwaidi.ae

ALSUWAIDI & COMPANY