Data Protection Considerations In UAE Related Arbitrations

Kluwer Arbitration Blog
August 6, 2020

Jane Rahman, Martin Hayward (Al Tamimi & Company)

Please refer to this post as: Jane Rahman, Martin Hayward, 'Data Protection Considerations In UAE Related Arbitrations', Kluwer Arbitration Blog, August 6 2020, http://arbitrationblog.kluwerarbitration.com/2020/08/06/data-protection-considerations-in-uae-related-arbitrations/

The data protection regime in the UAE is complicated. Parties to arbitrations that have connections to the UAE, regardless of whether the arbitrations are seated here, should be aware of the data protection regime(s) that may apply to them to ensure that no unintended breaches occur and to consider whether the relevant data protection regulations offer any strategic benefits for the dispute. In particular, parties should be aware that there are four different and distinct data protection regimes within the UAE. Onshore UAE has its own data protection regime and, in addition, the Dubai International Financial Centre (**DIFC**), the Abu Dhabi Global Market (**ADGM**), and Dubai Healthcare City (**DHCC**) each have their own data protection regimes.

The Data Protection Framework In The UAE

Onshore UAE

There is no single data protection law in onshore UAE. However, there is a broad and relatively far reaching concept of privacy that is protected and this has data protection consequences. Practitioners and controllers of data need to be alert to the different sources of law when ensuring compliance with data protection issues.

In brief, federal sources of law and regulation on data protection issues include:

• the UAE Constitution which, at Article 31, includes broad protections for privacy of communications;

• the UAE Penal Code which provides, at Articles 378 and 379, for criminal liability for certain breaches of privacy;

• the UAE Central Bank's Digital Payment Regulation (the Regulatory Framework for Stored Values and Electronic Payment Systems) which relates to digital payment service providers in the UAE;

• the Cyber Crimes Law (Federal Law No. 5 of 2012 on Combating Cyber Crimes) which (i) prohibits obtaining and dealing with certain information relating to medical data (Article 7); (ii) sets out certain prohibitions relating to financial information (Articles 12 and 13); and (iii) prohibits the use of information technology to violate the privacy of an individual or disclose certain confidential information (Articles 21 and 22); and

• the Law Regulating Telecommunications Sector (Federal Law by Decree No. 3 of 2003, as amended) which, among other things, establishes the Telecommunications Regulation Authority (the **TRA**) (Article 6) and provides that one of the TRA's competencies is the issuing of regulations regarding the use of subscribers' personal information (Article 14(3)).

In addition, Dubai has passed its own laws and regulations which may impact data protection. These include the "Dubai Data Law" (Dubai Law No. 26 of 2015 on the Regulation of Data Dissemination and Exchange in the Emirate of Dubai). Although the law is not a data protection law, it refers in general terms to data confidentiality and data protection. In addition, the Dubai Statistics Centre Law (Dubai Law No. 28 of 2015) protects personal data that has been obtained as confidential and limits how it may be disclosed or disseminated.

The net result is a patchwork of laws and regulations at the federal and emirate level that seeks to protect privacy through mandating and regulating how certain data is collected, stored, and shared. Breaches of the relevant UAE laws can lead to criminal and/or civil liabilities, imprisonment and/or fines.

For those involved in arbitrations that may involve data from or relating to this

region, consider whether any data in the arbitration:

• could be considered personal data because, for example, it relates to things such as a person's private or family life;

• relates to medical records;

• is user identification data or transaction records from digital payment service providers;

• is financial information and, if it is, whether it was properly accessed or obtained; or

• is subscriber information held by telecommunications providers.

If the data falls into any of these categories, it is worth taking advice early as it is likely there will be data protection issues to consider.

Offshore UAE

Three of the UAE's free zones, the DIFC, the ADGM, and the DHCC, each have their own data protection regimes. In addition, the UAE's criminal law uniformly applies across the country, including in the free zones. Accordingly, criminal liabilities relating to data protection (as discussed above) will be equally applicable in the free zones.

The DIFC's introduced a new data protection, Data Protection Law No. 5 of 2020, which came into effect on 1 July 2020. It replaced the previous data protection law, DIFC Law No. 01 of 2007.

The new law provides the DIFC with the most up to date data protection law across the UAE and its free zones. Key takeaways include that personal data may only be processed lawfully and in accordance with the new law (Section 9). In order for processing to be lawful, it must either be by consent or one of the other grounds must apply (Section 10). None of these grounds make reference to judicial or arbitral proceedings but, arguably, some of the grounds could be construed as to include judicial or arbitral proceedings. In addition, some categories of personal data (Special Categories) are afforded extra protections. So, personal data that

reveals or concerns "*(directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person*" must be treated with greater care. For such personal data, unless a data subject gives explicit consent to the processing of this personal data, it may not be processed unless one of eleven other grounds apply. One of these grounds is where the processing of the personal data is necessary "*for the establishment, exercise or defence of legal claims (including, without limitation, arbitration and other structured and commonly recognised alternative dispute resolution procedures, such as mediation) or is performed by the [DIFC] Court acting in its judicial capacity*" (Section 11(f)). It is not clear whether the legal claim must be one to which the data subject is a party or otherwise connected. There are restrictions on where certain personal data can be stored and/or transferred.

The ADGM's data protection law, the ADGM Data Protection Regulation 2015 (as amended), protects personal data in a similar fashion to the DIFC.

DHCC's Data Protection Regulation No. 7 of 2013 relates to patient health information. It introduces rules on what data can be collected: it must be necessary for a lawful purpose. However, "lawful purpose" is not defined in the regulations; how it must be stored; and how, if at all, it may be transferred and to where.

Those involved in arbitrations should consider whether the personal data:

• is patient health information;

• is personal data; or

• is sensitive personal data.

If it is any of these, it is worth taking advice early as there are more than likely to be data protection issues to consider.

Considerations For Arbitrations

Many aspects of a "standard" arbitration require the accessing, collection,

processing, storage, and dissemination of data. It is essential that all participants in an arbitration consider their own obligations in respect of data protection. Issues to consider include:

1. **The subject matter of the arbitration / identify of the parties** – Consider whether the subject matter of the arbitration or the identity of the parties mean that data protection issues may be more significant. For example, if a party to an arbitration is an individual this may give rise to immediate concerns in respect of the use of personal data. In addition, where the arbitration relates to health care companies, health care disputes, or health care data, there may be increased data protection obligations.

2. **Evidence in the arbitration** – Consider where the evidence is coming from and what it relates to as that may trigger data protection concerns. Think broadly about this. For example, if a strategy in an arbitration is to cast doubt on a witnesses' credibility and this entails searching for evidence of poor conduct on work emails, searching for and then dealing with such data may trigger some data protection considerations.

3. **Storage of and access to data** – Some data, in particular sensitive personal data, may have limits on how it may be dealt with. Think about what this means in practice including where relevant servers are located, whether cloud servers are used and, if so, where the cloud is "located", and who is accessing the relevant data and where they are based.

4. **Destruction of data** – What obligations (if any) arise in terms of the lawful destruction of data (e.g. data protection requirements for data minimisation) and who is responsible for ensuring compliance.

In practice, participants in arbitrations should:

• Think about data protection early and throughout.

• Identify relevant individuals with whom to liaise early.

• Establish as early as possible which data protection regimes may apply to your arbitration.

• Identify who in the arbitration may be a data controller under relevant laws and plan accordingly.

• Build data protection considerations into your arbitration.

Conclusion

The issues that may arise in respect of data protection are complicated and are likely to become more so. Consequences for lack of compliance can be serious. Relevant and early advice is essential. In addition, you should continually monitor data protection issues throughout the arbitration.