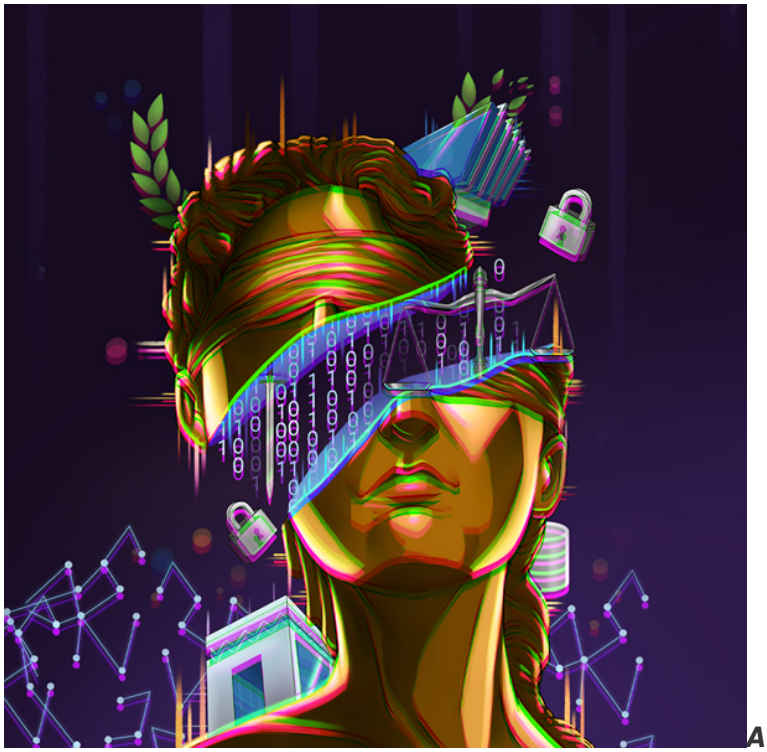
Data protection considerations in UAE related arbitrations

- Head of Digital & Data
- Dubai International Financial Centre

Martin Hayward - Digital & Data



A version of this article first appeared in [Kluwer Arbitration Blog](#) on August 6 2020.

There are four different and distinct data protection regimes within the UAE. Onshore UAE has its own (rather fragmented) data protection regime and, in addition, each of the following free zones have their own data protection regimes: (i) Dubai International Financial Centre ('DIFC'); (ii) the Abu Dhabi Global Market ('ADGM'); and (iii) Dubai Healthcare City ('DHCC').

Parties to arbitrations that have connections to the UAE or its free zones, regardless of whether those 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.

In this article, we briefly describe the different data protection regimes within the UAE, and we then consider some issues that parties to arbitrations connected to the UAE may wish to keep in mind as a result of the applicable data protection laws.

The Data Protection framework in the UAE

Onshore UAE

There is no single data protection law in onshore UAE. However, that does not mean that that there is no legislation relating to data protection in onshore UAE. In fact, there is a broad and relatively far reaching concept of privacy that is protected under various UAE laws and these have data protection consequences.

But it does mean that practitioners and controllers of data need to be more alert to the different sources of law that they must consider when ensuring compliance with data protection issues.

In brief, federal sources of law and regulation on data protection issues include: (i) the UAE Constitution (Federal Law No. 1 of 1971) which, at Article 31, includes broad protections for privacy of communications; (ii) the UAE Penal Code (which provides, at Articles 378 and 379, for criminal liability for certain breaches of privacy); (iii) 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; (iv) the Cyber Crimes Law (Federal Law No. 5 of 2012 on Combating Cyber Crimes) which, among other things, in Article 7 prohibits obtaining and dealing with certain information relating to medical data, where Articles 12 and 13 set out certain prohibitions relating to financial information, and in Articles 21 and 22, prohibits the use of information technology to violate the privacy of an individual or disclose certain confidential information; and (v) 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 some of its own laws and regulations which may impact data protection. These laws include what is known as the Dubai Data Law (Dubai Law No. 26 of 2015 on the Regulation of Data Dissemination and Exchange in the Emirate of Dubai) which requires that certain data that is held and which relates to the Emirate of Dubai is collated and managed and, in some cases, published as open data. Although the law is not itself 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 (not defined in the law) 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 levels that seek 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, some considerations include 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. If it is, then the person's consent may be needed before that data is dealt with;
- relates to medical records. If it does, then there may be limits on how that data can be dealt with;
- is user identification data or transaction records from digital payment service providers. If it is (and there is no definition of what constitutes user identification data), then there may be limits on how that data can be processed or shared and where and for how long it must be stored;
- is financial information and, if it is, whether it was properly accessed or obtained. If it is financial information and was unlawfully accessed in certain ways then criminal liabilities may arise depending on how that data is treated; and/or
- is subscriber information held by telecommunications' providers. If it is there may be obligations both on the telecommunications provider and any third parties who supply services to the subscribers on the telecommunications provider's behalf, to keep that information confidential and secure.

Offshore UAE

Of the UAE's many free zones, three (the DIFC, the ADGM, and the DHCC) 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 current data protection law, Data Protection Law No. 5 of 2020, came into effect on 1 July 2020. It replaces DIFC Law No. 01 of 2007, as amended.

The new law means the DIFC has the most up to date data protection law across the UAE and its free zones. A more detailed summary of the new law can be found here. Key takeaways include that, when the law applies, 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 applies. 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. Personal data is subject to relatively stringent controls and sensitive personal data is subject to extra protections. Personal data must be processed fairly, lawfully, and securely and for specified, explicit, and legitimate purposes. Again, as with the DIFC's law, the processing must either be by consent or one of the other grounds must apply. Similar to the DIFC's law, 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. Processing of sensitive personal data requires additional consent or one of the other grounds to apply. None of these grounds refer to judicial or arbitral proceedings or legal claims but, arguably, some could be construed to include these. There are also restrictions on where certain personal data can be stored and/or transferred.

DHCC has its own data protection regulation relating to patient health information (DHCC Data Protection Regulation No. 7 of 2013). The regulations introduce rules on what data can be collected: it must be necessary for a lawful purpose, though "*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 (including personal data from or relating to any of the DIFC, ADGM, or DHCC):

- is patient health information. If it is, there may be limits on how that data can be dealt with;
- is personal data. If it is, there are likely to be some restrictions on how that data is dealt with; and/or
- is sensitive personal data. If it is, then there are likely to be significant restrictions on how that data may be dealt with.

The application of UAE data protection laws

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 – arbitrators, parties, counsel and experts – consider their obligations in respect of data protection. Issues to consider include:

1. **The subject matter of the arbitration identity of the parties** – consider whether the subject matter of the arbitration or the identity of the parties mean that data protection issues may significant. For example, if a party to an arbitration is an individual (rather than an entity) this may give rise to immediate concerns in respect of the use of personal data in the arbitration. 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 whether that may trigger any data protection concerns. For example, where is the evidence that will be searched and potentially collected? Searching through hard copy company archives may pose different data protection issues as compared to searching through an employee's work computer. As a general rule, where you are contemplating searching through an individual's documents or devices, it may be pertinent to obtain advice as to any data protection issues that may need to be considered (including, without limitation to, whether employee consent has been obtained, either directly or indirectly). Similarly, consider what the evidence that you are searching for relates to and whether that may trigger any data protection concerns. Think broadly about this. For example, if a strategy in an arbitration is to cast doubt on a witness 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 well have limits on how it may be processed, transferred, or otherwise dealt with. Some UAE laws require certain data to be kept within the UAE or relevant free zone, or if transferred out of it, transferred only to certain jurisdictions. Again, think about what this means in practice. In particular, think about issues such as where relevant servers are "located": are they inside or outside of the appropriate jurisdiction? Is there any use of cloud servers and, if there is, where is the cloud "located"? Who is accessing the relevant data and where are they based? Consider both your own storage of and access to data but also how others will do the same: where, for example, will the tribunal store protected data that is shared with it?
4. **Destruction of data** – once the arbitration has come to an end, consider carefully 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.

Practical tips

In practice, participants in arbitrations should:

1. **think about it early and throughout** – consider data protection issues as early as possible both internally with your client and team and also, if appropriate, with your tribunal and opposing counsel;
2. **identify relevant individuals with whom to liaise early** – many clients will have individuals who are responsible for ensuring their company's compliance with relevant data protection laws. Identify these people early and work with them closely.;
3. **establish as early as possible which data protection regimes may apply to your arbitration** – take advice as early as possible as to which regime or regimes may apply to your arbitration so you can map out obligations early. With the potential for a new federal UAE data protection law in the near future, the UAE data protection landscape has the potential to either simplify or become increasingly complex;
4. **identify who in the arbitration may be a data controller under relevant laws and plan accordingly** – for example, is one or all of the tribunal a data controller and/or is the arbitral institution a data controller. If so, what does this mean for them and the arbitration?
5. **build data protection considerations into your arbitration** – consider raising data protection considerations during procedural hearings to ensure all parties and the tribunal have turned their minds to the relevant issues. In some instances, it will be appropriate to set out wording relating to data protection in procedural orders.

For further information, please contact Jane Rahman (j.rahman@tamimi.com) and Martin Hayward (m.hayward@tamimi.com).