

A New Electronic Transactions Law in the DIFC

Nick O'Connell - Partner, Head of Digital & Data - Saudi Arabia - Digital & Data
- Riyadh

The DIFC Electronic Transactions Law is primarily focussed on electronic contracts, electronic records, and electronic signatures. The purpose of the law is expressed as:

- to facilitate electronic transactions in DIFC;
- to eliminate barriers to electronic transactions resulting from uncertainties over writing and signature requirements;
- to promote the development of the legal and business infrastructure necessary to implement secure electronic transactions in DIFC; and
- to help to establish uniformity of rules, regulations and standards in DIFC regarding the authentication and integrity of electronic records.

In its July 2016 public consultation paper, the DIFC Authority explained that it wanted to clarify that, from a DIFC law perspective, electronic signatures are enforceable, electronic records are of the same effect as hard copies, and references to writing include writing by electronic means. Agreements made electronically would be as valid as those signed with 'wet ink' signatures, and electronic documentation would be treated as equivalent to paper documentation.

Electronic dealings, including dealings with the DIFC Authority, are already fairly common in the DIFC. By way of example, much of the DIFC company registration process, and associated licence renewal process, can be done on-line via the DIFC Authority's portal. The DIFC Authority acknowledges that there is little benefit in insisting on paper when parties are comfortable dealing electronically, and technology can bring with it similar, or greater, certainty than paper and wet ink.

With regard to electronic records, the DIFC Electronic Transactions Law provides that where any other DIFC law requires any record to be retained (or provides for certain consequences if it is not retained), that requirement is met by retaining the record electronically if certain conditions are satisfied. These conditions include: that the information contained in such record be preserved and capable of being reproduced in tangible form; that the record to be retained in the format in which it was originally created, generated, sent or received (or in a format that can be demonstrated to accurately replicate the information originally created, generated, sent or received); and that any details relating to the date and time, origin and destination and any sender or receiver be retained. Additionally, the law contemplates situations where authorities within the DIFC may specify compliance with certain other requirements relating to the retention of specific types of electronic records within their own areas of responsibility.

In its public consultation paper, the DIFC Authority noted that the draft law does not differentiate between different standards of secure and non-secure electronic signatures. It observed that most international legislation that includes such differentiation tends to attribute a higher evidential weight to electronic signatures that apply specified security procedures implemented by designated third party providers. In taking this approach, the DIFC Authority has avoided unnecessarily complicating the issue and negated the need to become involved in assessing and regulating a 'higher level' of electronic signatures.

In practical terms, prospective users of electronic signatures will, where circumstances require, be drawn towards electronic signatures that can be shown to utilise a higher level of technical security. Having a

legislated certification process for 'secure electronic signatures' (as is the approach taken in the UAE Federal Electronic Transactions Law) would not change this. (In our experience, the 'deemed reliability' outcome of the approach contained in the UAE Federal Electronic Transactions Law does not have particularly strong appeal in the market, particularly where international technology providers offering electronic signature solutions with a very high level of technical security have been reluctant to have themselves licensed as Certification Service Providers in the UAE.)

It should be noted that the DIFC Electronic Transactions Law contains significant exclusions in respect of the use of electronic records, electronic contracts and electronic signatures in the context of powers of attorney, wills and trusts, affidavits or affirmations and sale, purchase or long term lease of real property.

The DIFC Electronic Transactions Law is intended to be a framework for the recognition of electronic transactions, so it does not provide for penalties or sanctions. Other laws, such as the UAE Cyber Crimes Law and the UAE Penal Code, provide for penalties in respect of cybercrime type issues that may arise in the context of electronic transactions, and the DIFC Contract Law 2004 provides for remedies in the case of a breach of contract.

Al Tamimi & Company's Technology, Media & Telecommunications team regularly advises on electronic contracting, e-signatures, certification service provider issues, and other e-commerce related issues throughout the Middle East. For further information please contact Nick O'Connell (n.oconnell@tamimi.com) or Sana Saleem (s.saleem@tamimi.com).