

Electronic signatures in the UAE

Sana Saleem - Associate - Digital & Data
- Dubai International Financial Centre

September 2015

We have seen an increase in the number of enquiries from clients wanting use electronic signatures in their business processes in the UAE.

Some of the reasons for the limited adoption may be concerns about the following aspects:

- Does the law recognise an electronic signature as having legal force and effect?;
- What criteria should an electronic signature to meet in order to be enforceable?; and
- Is an electronic signature admissible as evidence in court in the event of a dispute between the parties to the agreement?

It is important to understand the legal framework in relation to the enforceability of electronic signatures before adopting electronic signatures for your business.

E-signatures in the UAE

In the UAE, the use and admissibility of electronic signatures is governed by Federal Law No.1 of 2006 regarding Electronic Transactions and E-Commerce (“Federal E-commerce Law”).

Basic electronic signatures are defined broadly to include all types of electronic signatures. These are generally defined as data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

An electronic signature that meets the requirements of the Federal E-commerce Law has legal force and effect under the Federal E-commerce Law. The Federal E-commerce Law further provides that nothing in the laws of evidence (which includes Federal Law No. 10 of 1992 (“Law of Evidence in Civil and Commercial Transactions”)) shall prevent the admission of an electronic message or e-signature in evidence.

Reliance on electronic signatures must be reasonable. Reasonableness is generally based on the following factors:

- the nature, value and importance of the transaction being supported by the electronic signature;
- steps taken by the relying party to verify the identity of the signatory of the electronic signature;
- evidence of prior breach or cancellation of the electronic signature;
- previous transactions between the parties, which relied on electronic signatures; and
- any other relevant factor.

There are, however, specific categories of transactions and documents for which electronic signatures may not be used, including:

- transactions and issues relating to personal law such as marriage, divorce and wills;
- deeds of title to immovable property;
- negotiable instruments;
- transactions involving the sale, purchase, lease (for a term of more than 10 years) and other disposition

- of immovable property and the registration of other rights relating to immovable property;
- any document legally required to be attested before a [Notary Public](#), and
- any other documents or transactions exempted by special provision of the law.

Secure e-signatures

The Federal E-commerce Law also provides for a 'secure' electronic signature for which there is a legal presumption of reliability. This may be contrasted with 'simple' electronic signatures for which no such presumption exists in law. Secure electronic signatures must be issued by recognised service providers in order to qualify as secure electronic signatures under the law.

Conclusion

It is important to bear in mind that electronic signatures are only as secure as the business processes and technology used to create them. High value or more important transactions need better quality electronic signatures – signatures used for these transactions need to be more securely linked to the signatory in order to provide the level of assurance needed and to ensure trust in the underlying system.

Al Tamimi & Company's Technology, Media & Telecommunications team regularly advises on e-signatures. For further information please contact Nick O'Connell (n.oconnell@tamimi.com) or Sana Saleem (s.saleem@tamimi.com)