



Things You Should Know About E- Signatures

April 2020

As business has moved online, we have been asked to verify the legality of various forms of digital signatures, including scanned signatures (including insertions into documents or copies of signed documents), “certified” signatures using programs such as Adobe Sign, creation of unique codes/QRs/number sequences generated by more complex programs, or even just emails with a person’s email signature.

The DIFC in 2017 issued an Electronic Transactions Law, DIFC Law No. 2 of 2017, which deals with electronic transactions and electronic signatures. The Law provides that electronic signatures are legally valid and enforceable in DIFC. The Law states that:

*“Where any provision set out in any other DIFC law requires the signature of any person, or provides for certain consequences if a document or a record is not signed, that provision set out in the other DIFC law is satisfied if an **Electronic Signature** is used.”*

The reference to DIFC law also includes the DFSA Rulebook.

An electronic signature is defined in the Law as:

“an Electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.”

The Law also mentions in which situations electronic signatures are **not** considered legal:

- a) The creation, performance or enforcement of a power of attorney.
- b) The creation, performance or enforcement of a declaration of trust (with the exception of implied, constructive and resulting trusts) and any provision in the Trust Law 2005 (DIFC Law No. 11 of 2005, as amended) requiring Information to be written or in writing.
- c) The creation and execution of wills, codicils or testamentary trusts.
- d) The creation, execution, and use of affidavits or affirmations as evidence in court proceedings pursuant to rule 29 of the Rules of the Dubai International Financial Centre Courts 2014.
- e) 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.”

In the public consultation paper issued prior to the Law’s enactment, the DIFC provided insight into the background for the introduction of the Law:

“DIFCA wishes to enact legislation to clarify for all purposes in the DIFC that electronic signatures are enforceable, that electronic records have equivalent effect to hard copies and that references to “writing” include electronic means.”

DIFC further noted that it does not wish to have a role in terms of regulating the use of which technology is considered secure in electronic communications, records, commerce or signatures as found in other legislation.

The law firm Al Tamimi and Company wrote the following in an article* regarding the new Law and the quality of the signature:

“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.)”

In conclusion, it is acceptable for client agreements and other documents relating to DFSA’s Rulebook (including AML and COB) to be signed electronically.

Where the rules explicitly require a “signature”, for example, the Client Agreement and Suitability Warning, at a minimum we would expect to see a scanned personal signature which can be verified against the signatures on passports and identity documents. Other correspondence with the client, including instructions for trading, may be subject to the Company’s internal risk assessment, and could simply include emails from verified email accounts, scanned documents, etc.

If you have any other questions, please do not hesitate to contact your Compliance Officer or any of the team at Capital Advantage.

References:

https://www.difc.ae/files/9714/9597/6158/DIFC_Electronic_Transactions_Law_No._2_of_2017.pdf

* O’Connell, Nick. “Electronic Transactions Law.” Al Tamimi and Company, 2016, www.tamimi.com/law-update-articles/electronic-transactions-law/.

<https://www.lexology.com/library/detail.aspx?g=89fdfce3-a3e7-496a-9477-a39c4a770905>