Baker McKenzie.

Client Alert
April 2020

COVID-19 IN THE MIDDLE EAST

Executing contracts electronically: a practical guide

In the wake of the COVID-19 health crisis, working-from-home has become the new normal, however, it does present a number of practical challenges, including how to execute legally binding documents. It has long been common practice for deal documents to be signed in counterpart, on different days, by signatories in different corners of the globe, but with our freedom of movement curtailed and home printing capabilities limited, feasible options are often restricted.

Electronic contract execution offers a convenient solution but their penetration in the Middle East is lower than in some other parts of the world, notably North America and Europe. In this alert, we consider the key practical considerations for businesses thinking of adopting an electronic execution process, including when it is appropriate to do so, and how to improve the enforceability of contracts signed in this way.

This alert provides high-level guidance on the issues raised by electronic contract execution and is not a substitute for tailored legal advice, which takes into account the facts specific to your business and its need.

Checklist

In summary, the key steps that businesses should take when executing documents electronically are as follows:

1. Confirm that exchanging signatures electronically and maintaining an electronic record are permitted under the law governing the contract.

2. Confirm that the parties have agreed to exchange signatures electronically and maintain an electronic record of this – the simplest approach may be to include language to this effect in the contract or in the execution instructions.

3. Confirm that the type of document is not one that is exempted from being validly executed electronically (*e.g.* power of attorney, negotiable instrument, or document that requires notarisation).

4. Confirm that the constituent documents of the signing organisations do not restrict the use of e-signatures, or dictate mandatory requirements to authorise their use (*e.g.* board

resolutions).

5. Choose a desired method for exchanging signatures, which satisfies the requirements of the law.

The laws in the Middle East generally recognise the validity of e-signatures and tend to be technology neutral (i.e. not prescriptive regarding the form of the e-signature). However, in some jurisdictions, certain types of electronic signatures are presumed valid if they comply with a certain set of requirements imposed by local laws. Generally, for an e-signature to be relied upon, it must be capable of accurately verifying the identity of the signatory. Once an e-signature has been affixed to a document, it should be date stamped and incapable of being amended. Only an e-signature solution which satisfies this threshold will be enforceable if the validity of the e-signature is challenged.

In detail: Determining whether a contract can be signed and delivered electronically

1. The law of the contract

The threshold question is whether the governing law of the contract supports electronic contract execution. Broadly speaking, under the laws of the Gulf Cooperative Council (**GCC**) and Egypt, e-signatures have the same legal effect as hand written, wet ink signatures, provided that the relevant requirements of the local law are met (*e.g.* that the signature can be relied upon to verify the identity of the user).

A. Examples of e-signatures

In practical terms, subject to the other considerations noted below, the following e-signature methods are commonly used:

- The "sign and scan" approach, where parties sign, scan, and affix a signature page to a soft copy of a final contract;
- Digital signature software, which tends to provide a comprehensive means of collecting, storing and affixing digital signatures and which are designed to satisfy common legal validity requirements; and
- Stating your intention to be bound to a contract over email or using another electronic communication platform (*e.g.* click acceptance of "I agree" or "I consent").

Notably, not all of these methods are equal and it will be challenging to verify the identity of the signatory and demonstrate that reliance placed on the electronic signature is reasonable for some of them. These methods would also need to be adopted as part of a more comprehensive signing protocol, with additional safeguards built in. The process may also need to be more rigorous when signing deal documents as opposed to more routine, nominal value and/or internal documents.

B. Verification

To increase the likelihood that an e-signature can be relied upon, generally speaking parties should use an e-signature solution that enables them to:

- verify the identity of the signatory;
- verify that the e-signature has been affixed by that signatory (*e.g.* a procedure that safeguards against unauthorised access or use of the e-signature by anyone else); and
- ensure that once signed, the document has not been altered or tampered with (*e.g.* a system which creates an immutable record and enables the parties to detect when and where any subsequent changes are made).

The more robust the verification process, the more likely that the e-signature will be enforceable if its validity is challenged in court proceedings.

In theory, one way to approach this issue would be to have the e-signature supported by an electronic attestation certificate, which confirms the identity of the person or entity which administers the e-signature. These certificates must be issued by a certified provider (*e.g.* a person or organisation which is formally accredited or authorised to issue digital trust certificates).

In Saudi Arabia, digital certification services are provided by certification service providers which are licensed by the Communications and Information Technology Commission. Licensed certification agencies also exist in Egypt, or the Information Technology Industry Development Authority can verify electronic signatures. However, these services are not always available. As a case in point, the UAE currently has no formally accredited bodies that issue electronic attestation certificates.

C. Electronic records

The laws of the GCC states and Egypt generally provide that, except for certain types of contracts, a contract or record will not be denied legal effect or enforceability solely because it is in electronic form. Therefore, exchanging soft copies of documents electronically will not affect the validity of the underlying document and that if the law stipulates that a 'record' must be in writing, an electronic record is acceptable.

In practical terms, the types of electronic records which are generally used include:

- compiled PDF soft copy documents;
- duplicate copies or printed versions of hard copy documents;
- records retained on a USB or CD; and
- emails that have been downloaded,

provided in each case the records meet the requirements set out in the law.

In the UAE and Saudi Arabia, for example, the electronic record:

- must be saved in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

- must be stored in a way that is accessible and usable to allow for subsequent reference; and

- with reference to emails in particular, must be kept in a way that enables the identification of the origin and destination of an electronic message and the date and time when it was sent or received.

2. Agreement to use electronic signatures, delivery and retention

Subject to express restrictions in the applicable law, parties are generally free to negotiate terms to permit or prohibit concluding a contract electronically. Before exchanging signatures by email, the specific terms and conditions of a contract should be reviewed to confirm whether parties have consented to the use of e-signatures and records.

3. The subject matter of the contract

Before electronically signing documents, it is critical to check whether the document is capable of being validly executed using an electronic signature. Generally speaking, the laws of the GCC provide a valid legal basis for the use of electronic contracts and digital signatures, and most contracts can be effectively executed using e-signatures. However, certain categories of documents are expressly exempted and will not be valid if signed electronically.

In the UAE, these include:

- documents related to personal legal matters such as marriage, divorce and wills;

- transactions concerning the sale and purchase and disposition of real estate or their lease for a period longer than ten years and the registration of any relevant rights;

- negotiable instruments such as bonds and bills of exchange; and

- any document legally required to be attested before a Notary Public (this includes UAE corporate authorisations such as powers of attorney, resolutions and certain security documents governed by UAE law provided in financing transactions).

4. Other considerations

Some other considerations for determining whether a contract can be signed and delivered electronically include the following:

- Where a contract is being signed on behalf of a legal entity, whether the articles and by-laws governing the internal affairs of that entity restrict the entity from entering into an agreement by

e-signature. Most governing documents do not expressly prohibit the use of e-signatures; however, it is important to verify that the chosen signature approach does not contradict the entity's governing documents.

- Where a document needs to be filed with a government department, whether the rules which govern this process mandates, or in practice requires, submission of hard copy, wet ink signed documents.

- Whether the document needs to be notarised in order to satisfy other applicable legal formalities, a process which is generally carried out in person using hard copy original documents.

- Whether for tax purposes the document should be signed in a specific location, in order to avoid any undesirable tax treatment of the underlying transaction.

For further information, please feel free to contact one of the lawyers below or your usual Baker McKenzie contact.

This alert is prepared by Kellie Blyth (Head of IT & Communications, Dubai); Sandeep Puri (Head of Banking & Finance, Dubai); Farah Abed (Associate, Banking & Finance, Dubai); Hani Naja (Partner, Corporate, Abu Dhabi/Dubai); Tala Shomar (Associate, Corporate, Dubai); Eby Oligboh (Trainee Solicitor, Dubai); Zahi Younes (Partner, Corporate, Riyadh); Ghada El Ehwany (Partner, Corporate, Cairo); and Moataz El Sherbini (Associate, Corporate, Cairo).

Contacts

Kellie Blyth
Head of IT& Communications
Dubai
Kellie.Blyth@
bakermckenzie.com

Zahi Younes
Partner, Corporate
Riyadh
zahi.younes@
legal-advisors.com

Ghada El Ehwany
Partner, Corporate
Cairo
Ghada.ElEhwany@
bakermckenzie.com