HR Electronic Records

Electronic Signatures in United Arab Emirates: What it means for HR

What is an electronic signature?

Generally speaking, an electronic signature (or e-signature) is a technical process logically associated with a document which two (or more) individuals or organizations (the signatories) agree to rely on in order to express their intent to sign such document. Three components are therefore necessary: a document, a signatory and an e-signature tool. While the tool most commonly used for handwritten signatures is a simple pen, electronic signature tools are typically more complex. From a regulatory standpoint, an electronic signature is a broad category that encompasses many types (or levels) of electronic signatures.

Depending on the country it is used in, there are differences in purpose, legal acceptance, technical implementation and cultural acceptance of electronic signatures. In particular, e-signature requirements tend to vary significantly between most "civil law" countries (including the European Union and many countries in South America and Asia), and most "common law" countries (such as the United States, Canada and Australia). Civil law countries typically support a "tiered" approach including higher levels of signature often called digital or qualified electronic signatures (typically required for specific types of contracts), as opposed to common law jurisdictions which are typically more technology-neutral. In addition, some industries (such as healthcare or banking) and documents (such as marriage or adoption contracts) may require a higher level of e-signature.

What are the laws and regulations in the United Arab Emirates?

Electronic signatures are recognized under Federal Decree-Law No. 46 of 2021 On Electronic Transactions and Trust Services. Under Article 8 of this Law, if a signature is legally required, a reliable electronic signature can be used, as long as the signature meets certain requirements.

The Law distinguishes between two types of electronic signatures:

Qualified Electronic Signatures must:

- be completely and exclusively associated with the signatory and under their control.
- have the characteristic of identifying the signatory.
- be linked to the data signed in a way that any modification to that data can be discovered.
- be created with technical and security techniques in accordance with the technical requirements specified by the Implementing Regulation of the Law; and,
- other conditions specified by the Implementing Regulation of the Law.

Approved Electronic Signatures are Qualified Electronic Signatures that have been created with a tool on the Telecommunication and Digital Government Regulatory Authority's (TDRA) approved list and issued based on an Approved Electronic Signature Authentication Certificate.

The Law also defines an "**Electronic Stamp**" (i.e., data in electronic form, connected or logically linked to an electronic document used to confirm the identity of the person and the origin and integrity of the data source in that document). Qualified Electronic Stamps and Approved Electronic Stamps are distinguished in a way similar to Electronic Signatures.

Is an electronic signature valid in the United Arab Emirates?

Electronic signatures are valid, per the Law of Evidence. The electronic signature needs to meet the requirements under the Law to be considered valid.

Federal Decree-Law No. 46 of 2021 On Electronic Transactions and Trust Services permits any document to be signed electronically and hold the same weight as a wet ink signature unless a specific law states otherwise. Federal Decree-Law No. 33 of 2021 On Regulation of Labour Relations (the Labour Law) does not contain an exemption to the validity of electronic signatures.

Electronic Signatures and Electronic Stamps are considered 'valid' if they meet certain conditions:

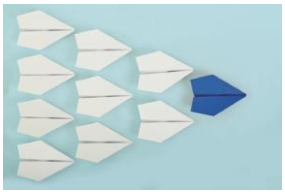
- They were created based on an approved and valid authentication certificate.
- They were created using an Approved Electronic Signature or Stamp tool.
- The data to prove the authenticity of the Approved Electronic Signature and the Approved Electronic Stamp is identical to the data submitted to the relying party.

- The data identifying the signatory of the authentication certificate has been submitted to the relying party.
- They are created with technical and security techniques to be specified in the implementing regulations of the Law.

Ultimately, the employer (or other party) who relies on electronic signatures bears the obligation of verifying its validity and authenticity, and is liable for the consequences if the electronic signature is invalidated.

For an employer or other relying party to trust and rely on the Electronic Signature or the Electronic Stamp, it must take into account:

- the security level of the Electronic Signature or Electronic Stamp according to the nature, value or importance of the transaction;
- take necessary measures to verify the identity of the signatory and the validity of the authentication certificate;
- take necessary measures to verify that the Electronic Signature or the Electronic Stamp satisfies the validity requirements imposed by the Law;
- to the extent of its knowledge or presumed knowledge, the Electronic Signature, Electronic Stamp, or electronic authentication certificate has not been breached or withdrawn; and,
- have consideration to previous agreements or dealing between the signatory and the relying party where the parties have relied on Electronic Signatures, Electronic Stamps, or authentication certificates.



HR Best Practices

Contracts may not be denied validity or enforceability solely for being concluded in one or several electronic messages. Electronic signatures are generally valid in the employment context, as long as they follow the requirements under the law.

Last updated September 2022.