Electronic execution of contracts, e-signatures and COVID-19: Spain

by Andy Ramos Gil de la Haza and Álvaro Martínez Crespo, PÉREZ-LLORCA

Articles | Published on 29-Jul-2020 | Spain

This article discusses the electronic execution of contracts and the validity of e-signatures under Spanish law in the context of the 2019 novel coronavirus disease (COVID-19) pandemic.

The crisis caused by the 2019 novel coronavirus disease (COVID-19) pandemic has had repercussions on the execution of corporate and commercial agreements by legal entities. To formalise their business relationships, many companies have been forced to move from traditional wet ink signatures to the use of e-signatures. However, the existing regulations have not been amended, and there is currently no legal framework addressing e-signatures in Spain.

Main requirements for a legally binding contract

Similar to other countries with a civil law tradition, the Spanish Civil Code provides that, for an agreement to be legally binding, it must contain three essential elements:

- Mutual agreement between the parties.
- An identifiable object.
- Consideration.

In Spain, the principle of "freedom of form" applies to contracts (*Articles 1278-1280, Civil Code*). The Supreme Court has stated on different occasions (see for example *STS, S.1ª, 22-IV-2013, rec 505/2010*) that this is the general rule of the Spanish contracting system. Written and verbal agreements are allowed, with a few exceptions (such as the assignment of intellectual property rights) where the written form is required, not only for proving the document's existence in court (*ad probationem*), but also for its execution (*ad solemnitatem*). In any case, electronic documents do qualify as written agreements, and therefore no tangible form is required.

Is any particular form required by law?

There are some exceptions that prevent the signing of certain agreements using e-signatures. This is the case for specific types of agreement, which must be drawn up as a deed, or registered in the relevant register. For example:

- Documents related to family law or inheritance must be notarised.
- Contracts for the purchase, lease or transfer of real estate, and donations of real estate must be made by deed (*Article 633, Civil Code*).

- Mortgage agreements must be registered with the Land Registry (*Article 1875, Civil Code*).

Apart from these exceptions, the signing of contracts by electronic means is permitted, as long as the parties agree to employ this method (according to the *pacta sunt servanda* principle), whether by using a digital certificate, an electronic national identity card or a "trust service provider". A trust service provider is a natural or a legal person which provides one or more trust services either as a qualified or as a non-qualified trust service provider (*Regulation 910/2014* (e-Idas Regulation)). The parties to an electronic contract can agree to sign the document through a trust service provider (*Article 25, Law 34/2002 on Information Society Services and Electronic Commerce*).

The e-Idas Regulation and Law 59/2003 of 19 December 2003 on e-signatures provide that e-signatures and certification systems, such as those used by AdobeSign, DocuSign and so on can be used and are recognised in Spain under the principle of freedom of form. A draft piece of legislation currently under consideration by parliament (on Certain Aspects of Trusted Electronic Services), would fully repeal Law 59/2003, while developing different elements of the e-Idas Regulation, including the verification of the identity and attributes of applicants for a qualified certificate, the sanctioning regime and the conditions for the suspension of certificates.

The parties to an agreement can use the trust service providers that comply with the provisions of the e-Idas Regulation, and specifically those services relating to e-signatures, electronic seals and electronic time stamps.

What is an e-signature?

Under the e-Idas Regulation there are three types of e-signature:

- **Simple.** This is where data in electronic format, which is attached to other electronic data or is logically linked to it, is used to sign a document. Examples of simple e-signatures are acceptances of terms and conditions by checking a box, or a handwritten signature which is scanned and inserted into an agreement. This type of signature provides little guarantee as to the person who has actually supplied it.
- **Advanced.** This type of signature must be:
    - uniquely linked to the signatory;
    - capable of identifying the signatory;
    - generated using electronic signature creation data that the signatory can, with a high level of confidence, use under their sole control; and
    - linked to the undersigned data in such a way that the receiver of the document would be able to detect any subsequent alterations to the document.

    These conditions may be satisfied, for example, by requiring the signatory to enter a PIN number received on their mobile phone during the signing process.
- **Qualified.** This is an advanced e-signature created by a specific device and based on a qualified certificate for electronic signatures.

Under the e-Idas Regulation, only the qualified e-signature has the same legal effect as that of a handwritten signature, and is valid in all EU member states.

This does not mean that simple e-signatures and advanced e-signatures have no legal validity, but rather that their legal validity will not be presumed in legal proceedings in the same way as that of a handwritten signature.

Business try to strike a balance between efficiency and legal certainty, by using simple or advanced e-signatures for most transactions (supported by other information, including qualified time stamps) while using qualified e-signatures only for larger deals. Before opting for one technology and service over another, it is advisable for the parties to discuss the options and agree how best to execute contracts electronically.

Using any electronic or traditional document signature system runs the risk of identity theft by employees, collaborators or any third parties who have access to the e-signature, the physical document, the signatory's email or a scanned signature.

If a handwritten signature is forged, the claimant's only recourse is to employ a handwriting expert to prove that the signature has been falsified. However, in the case of a forged e-signature, the claimant will have (as long as a trust service provider is involved) various data at their disposal, such as the tracking of the transaction (with time stamps, IP addresses, signature devices and so on) and even an unaltered copy of the document saved in the trust service provider's system.

Court admissibility

A simple or advanced e-signature or electronic seal may be admissible in legal proceedings if it is accompanied by sufficient information to allow the court to establish that the document conveys the willingness of both parties to enter into the contract. The burden of proof is on the party seeking to enforce the e-signed documents.

Entities that choose to use simple or advanced e-signatures (currently the most commonly used) should include, where possible, a time stamp or technical data relating to the signatories, their devices and IP addresses. This will strengthen a document's admissibility in legal proceedings.

Legal developments in light of COVID-19

The COVID-19 pandemic has not had a significant impact on the use of e-signatures to formalise corporate and commercial agreements, although there have been legal changes in relation to documents processed by the public administration (see below).

The e-Idas Regulation recognises, throughout the EU, qualified e-signatures (but not simple and advanced e-signatures) that are based on a qualified certificate and issued in a member state. However, parties should check the requirements for and restrictions on the use of e-signatures in the individual member state, as local registries and regulators may have amended their rules about the execution of documents, and companies may have introduced additional restrictions on e-signatures in their by-laws.

Royal Decree 463/2020 and Royal Decree-law 11/2020 introduced a series of extraordinary measures designed to deal with the new circumstances of the COVID-19 pandemic. The measures relate, among other things, to the issue, renewal, expiry and validation of electronic certificates by public bodies.

E-signature certificates that have expired or are about to expire, along with new certificates, normally require renewal or issue in the presence of the certificate holder or their legal representative. However, the National Currency and Stamp Manufacturer and the Spanish tax authorities have made the renewal of these certificates more flexible. They have also permitted the use of expired certificates or certificates which are about to expire on or after 1 February 2020.

Royal Decree-law 11/2020 introduced provisional measures for the issue of new qualified certificates. It permits the issue of certificates that have been qualified remotely, as long as the certification entity follows the Authorisation of Remote Identification Procedures by Video Conference. This was published on 12 February 2016 by the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences. The certification entity must, among other steps:

- Carry out a specific risk analysis.
- Document the qualification procedure and test its effectiveness.
- Implement technical requirements designed to ensure the authenticity and validity of the identification documents used by the signatory.
- Record the identification process with a time and date stamp.

END OF DOCUMENT