ELECTRONIC SIGNATURE

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.

What are the laws and regulations in India?

The Information Technology Act includes three types of e-signatures: (1) electronic signatures; (2) digital signatures; and, (3) electronic documents executed with free consent by any other means, in accordance with the principles of contract law.

Electronic signatures must be considered reliable and be specified in the Second Schedule of the Information Technology Act. To be considered reliable:

- the authentication/creation data used must be linked to the signatory;
- the authentication/creation data must be under the control of the signatory (at the time of signing) and no other individual; and,
- all changes/alterations to the signature and the data must be detectible after signing.

At this time, the only electronic authentication technique specified is Aadhaar e-KYC services. Under Aadhaar e-KYC services, a signature is linked with the individual's Aadhaar (a unique identity number issued to Indian residents) and a One Time Password (OTP) is generated. The individual can then use this signature to electronically sign documents.

Digital signatures employ asymmetric crypto systems and hash functions which have been issued by a licensed certifying authority. These are usually used for corporate regulatory and taxation filings.

To authenticate electronic signatures or digital signatures under the Information Technology Act, a licensed Certifying Authority would need to validate the signature and issue either an

Electronic Signature Certificate (ESC) or a Digital Signature Certificate (DSC).

There are some documents which cannot be executed electronically, including negotiable instruments, Powers of Attorney, trusts, wills and documents relating to sale/conveyance/interest in immovable property.

Free Consent: A third valid method is to execute an electronic document in any manner that involves free consent (ex., a clickwrap contract). If this method is questioned, the employer (i.e. the concerned party), would need to provide evidence that the employee actually signed or provided free consent to the relevant document.

Is an electronic signature valid in India?

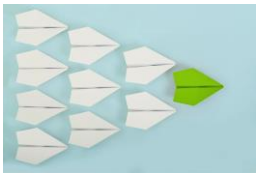
Yes, HR documents can be executed using electronic signatures. Theoretically, there is no difference between electronic evidence of a contract executed electronically and a paper contract executed with a wet-ink signature. In practice, employers who rely on an electronic document must be able to prove that the following conditions are being met:

- the output being produced by a computer regularly used to store/process information by the person who has lawful control over the computer;
- during the period the record was created, data similar to the information contained in the electronic record has been regularly entered into the computer (i.e. the record in evidence was managed in the same way other records were managed);
- the computer operating properly through the material part of such period (or, if the computer was not working properly, the non-operation did not impact the accuracy of the record or its contents); and,
- the electronic record containing or being derived from information entered into the computer in the ordinary course of activities.

To be admitted as evidence, electronic records must be accompanied by a certificate which:

- shows the conditions above were met;
- identifies the electronic record containing the statement;
- describes the manner in which the record was produced;
- provides the details of the device involved in the production of the electronic record to show the record was produced by a computer; and,
- is signed by an individual in a responsible official position relating to the operation of the device or the management of the relevant activities.

The above referenced certificate must be prepared by the party in control of the electronic document/device.



HR Best Practices: In theory electronic and wet-ink signatures can generally have the same legal value. In practice, the evidence of a contract executed electronically in India may have marginally less value due to the added conditions that must be satisfied.

Last updated June 2021.