

Ready for your company's digital transformation by starting with E-signature?



ASIA

— the Legal Environment of E-signatures in China

Under the impact of COVID-19, the travelling and face-to-face meeting encounter difficulties. More and more enterprises, especially the transnational enterprises, are exploring the feasibility of electronic contracts ("E-Contracts") with electronic signatures ("E-signatures").

Unpredictably, the beginning represented by the epidemic situation has laid a keynote of «Digital Year» for 2020. The online government affairs and online offices promoted by non-contact are called the new normal in the post epidemic era.

In such era, the e-signature industry, which has always kept a low profile, has ushered in its own highlight moment. In addition, under the new normal, new fields such as online health care, online education, online banking business, strongly boost the development of the e-signature industry. With the digitalization of business in all walks of life, e-signatures will gradually become one of the underlying infrastructure of the whole commercial world.

Here we will briefly introduce some main concepts of e-signature mechanism under Chinese legal environment.

■ WHAT IT IS AN E-SIGNATURE?

The e-signature is not the signature or seal what we usually see in a printed document. It is more than the signature and/or seal showed on an electronic document ("E-document") and actually consists of a series of data.

The *E-Signature Law of the PRC* (initially passed on August 28, 2004, and recently modified on April 23, 2019) defined the "E-signature" as "data contained in or attached to a data message in electronic form, which is used to identify the signatory and indicate the signatory's approval of the content therein." Thus, essentially, e-signature is data. It is the key to understand how an e-signature works.

■ IS THE FORM OF E-CONTRACT USING E-SIGNATURE RECOGNIZED UNDER CHINESE LAWS?

The answer is positive. The *Contract Law of the PRC* provides that the parties may conclude a contract in written, oral or other forms, and the written form includes electronic data.

Therefore, e-contract is recognized under the Chinese laws and constitutes an effective written form of contract. Normally e-contracts in electronic form executed with reliable e-signatures are with legal effect, but when the form changes its legal effect would be changed as well. For example, if you print out an e-contract signed with the e-signatures by parties, such hardcopy itself has no legal effect and can only serve as a copy, instead of the original (the e-contract in electronic form). This is almost contrary to the traditional practice where parties execute contracts with signatures made by hand.

■ CAN ANY E-DOCUMENT BE LEGALLY ACCEPTED TO BE EXECUTED WITH E-SIGNATURE?

Obviously no. The *E-Signature law of the PRC* provided two pre-conditions for the adoption of e-signatures:

1. Free will of the civil parties involved;
2. Exclusion of three types of contracts:
 - documents relating to personal relationships such as marriage, adoption and inheritance;
 - documents involving suspension of public utilities such as water supply, heating supply, gas supply etc.; or
 - any other circumstances where electronic documents are not applicable as stipulated by laws and administrative regulations.

In conclusion, if it is not related to personal relationship, suspension of public facilities or other domains restricted by the laws, the civil parties could voluntarily decide that they shall resort to electronic signature and data message for documents or not.

■ DOES ANY E-SIGNATURE HAVE THE SAME LEGAL EFFECT AS THE HANDWRITING SIGNATURES?

Per the *E-Signature Law of the PRC*, only "reliable" e-signatures shall have the same legal validity as handwritten signature or affixation of seal. So what is a "reliable" e-signature then?

According to the *E-Signature Law of the PRC*, parties to an e-document may freely decide conditions to be fulfilled for a "reliable" e-signature, on the premises that their e-signatures shall meet the following four legal criteria (minimum mandatory criteria):

1. when the e-signature creation data is used for e-signature, it is exclusively proprietary to the electronic signatory;
2. the e-signature creation data is exclusively controlled by the electronic signatory at the time of signing;
3. any subsequent alteration to the e-signature after the signature can be detectable; and
4. any subsequent alteration to the content and form of the data message after the signature can be detectable.

The first two criteria are used to prove the identity of the signatory and the last two criteria are used to prove the secured content and integrity of the e-document with the e-signature.

In practice, as the four criteria are abstract, companies rely on third party to authenticate the e-signature. In China, only the legitimate electronic authentication service provider (also referred to as Certificate Authority, "CA") could provide this authentication service. A qualified third-party CA will issue the electronic certificate ("**CA certificate**") for the signatory to prove a reliable e-signature. The CA certificate may serve as a "data ID" for the corresponding e-signature.

■ RECOGNITION OF E-SIGNATURE IN JUDICIAL PRACTICE

In the judicial practice of China, when the validity of an e-signature is challenged in a litigation, the Chinese court usually evaluates the validity of the e-signature from the following aspects: whether the signatory is properly identified during signing process, whether the e-document, as well as the e-signature has been altered, whether there is other proof (i.e. CA certificate, trusted time stamp which proves the time when the e-document is signed, block chain technology and etc.) justifying the validity of such e-signature.

CA certificate issued by a Chinese qualified CA in China is generally recognized and accepted by the court to support the "reliability" of an e-signature. Recently in China, block chain technology has also started to be recognized by the court, especially by the Internet court.

For international groups, the foreign headquarters prefer to use a foreign e-signature service provider, but is concerned about its validity under Chinese judicial system. Article 26 of the E-Signature Law has mentioned this approach: *Upon verification by the information industry department of the State*

Council in accordance with the relevant agreement or reciprocity, electronic signature certificates issued overseas by foreign electronic authentication service providers shall have the same legal validity as electronic signature certificates issued by electronic authentication service providers established pursuant to this Law.

However, in practice, it seems that only few foreign e-signature providers have been legally recognized in China in the past. Thus, considering the current judicial practice, there are still risks where such e-signature service is provided by a foreign provider, which would not be recognized by the court. In particular, in cross-border E-commerce, the situation is always complicated because different countries/regions have their own legal requirements on e-signatures, so issues may be raised during the identification of different signatories under different jurisdictions. Then, the coordination of two or more different legal and judicial systems may be involved, and the legal validity of the e-signature provided by a foreign provider would be uncertain. Therefore, for the issues to be solved within the territory of China, we would recommend a qualified Chinese e-signature service provider to avoid that the e-contracts or other e-documents being deemed as non-valid.

■ TREND OF APPLICATION OF E-SIGNATURE IN CHINA

The Chinese government has encouraged the application of e-signature during the recent years. The e-business license of enterprises has been launched years ago, and the e-labor contract has been officially recognized by the Ministry of Human Resources and Social Security in March this year 2020.

In some cities, local administrative regulations have been issued regarding the application of electronic seals ("E-seal") of enterprises, which has been recognized as one form of the e-signature. E-seals of a company may include electronic company seal, legal representative's seal and even financial seal. In Beijing, the application of e-seal shall be made by the authorized entity and registered at the local public security bureau; while in Shanghai, an official platform has been established by the local Administration of Market Regulation for the issuance, storage and use of e-seal. However, similar to the physical company seal, the e-seal shall also be controlled properly to avoid illegal access and misuse.

With the e-seal, companies may execute e-documents on the designated official platform and submit the required e-documents to the relevant authorities. It is different from submitting scanned copies of signed/chopped documents online as sometime currently required/accepted by some authorities. When an e-document attached with an e-seal and other forms of e-signature (such as the e-signature of president of a company) is accepted, there is no longer hard copies of the document. However, even though the official platform of e-seal has emerged, the use of e-document with e-signature in administrative formalities is still quite limited. When the internal decision of a company, such as Board's Resolution or Shareholders' Resolution, is needed for administrative registrations, a hard copy with handwriting signature of the directors or legal representatives shall still be submitted in most cases. Therefore, in administrative matters, we still rely on the feedback of correspondent authority regarding the possible use of e-document with e-signature. However, we believe that with the development of digitalization of Chinese government affairs, the e-document may be accepted in order to lift the burden of enterprises on administrative formalities in the near future.

■ IMPORTANCE OF DATA SECURITY IN APPLICATION OF E-SIGNATURES

The application of e-signature is not an isolated decision in the management of a modern and compliant company. The data security plays a significant role in this mechanism, while all enterprises are concerned about data security issue, especially the contractual transaction data related to the core business of enterprises.

For example, should the internal rules fail to strictly manage the e-signature creation data, companies may suffer losses and even civil liabilities. One case to this point could be that, where a company's previous legal representative still uses the e-signature representing the company to execute commercial

contracts, and such company fails to inform the relevant parties about the replacement of its legal representative or properly keep the e-signature creation data with its new legal representative. In such case, the e-signature used to represent the company could be still considered as "reliable" and the contracts concluded be therefore valid.

Besides, as the "uniqueness" of the data consisted in an e-signature, when the e-signature is no longer confidential or no longer identifiable (such as the e-signature creation data (i.e. a U-key) is or may be used by unauthorized entity), the correspondent signatory shall inform the relevant parties and terminate the use of such e-signature. The obligation to safeguard the e-signature data is also cleared stated in the *E-signature Law of the PRC*. Failing to fulfil this obligation will lead to civil liabilities associated with such e-signature creation data. For instance, the contractual liabilities concluded with unauthorized use of such e-signature creation data.

In order to safely use the e-signature, an enterprise shall also evaluate whether its IT infrastructure and policies could meet its business needs. As required by *the Cyber Security Law*, a certain series of internet security protection obligation shall be fulfilled to prevent internet invasion and unauthorized access, such as technical measures to prevent computer virus, network attacks, network intrusions and other activities that endanger cybersecurity, to monitor and record network operation and cybersecurity events, data classification, as well as the backup and encryption of important data.

Therefore, we suggest that enterprises that choose to use e-signature should pay special attention to its internal rules and IT capability regarding the data security.

■ DS RECOMMENDATIONS

To sum up, we have the following recommendations for your understanding and preparation of e-signature in China:

1. Make sure that the type of legal documents using E-signatures DO NOT fall into the three categories of documents where the E-signature is prohibited;
2. Reach a mutual written consent on using E-signatures with the relevant party, and specify the mutually agreed conditions for a reliable e-signature;
3. Select a qualified Chinese e-signature service provider to use and verify the e-signatures;
4. Consult professionals to establish internal rules and IT capability for the compliant and secured use of e-signatures, especially e-seals.

Under such post epidemic era, there is an increasing number of enterprises resort to e-signatures. In particular, a company may have to adopt it when its upstream and/or downstream partners start to use e-signatures. It is also called "chain effect" in the commercial world. Therefore, we suggest that companies start to be ready for the use of e-signature, both from legal aspect and technical aspect, so as to avoid being left in the trend of digital transformation.



For any additional information
please contact:

WANG Fanglei
Associate - Beijing Office
wangfanglei@dsavocats.com

ZHANG Beibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com

To unsubscribe, click [here](#)