Electronic Signature Law of the People's Republic of China

March 2019

ASIA BRIEFING

DEZAN SHIRA & ASSOCIATES
Your Partner for Growth in Asia

Source: National People's Congress, http://www.npc.gov.cn/englishnpc/Law/2007-12/05/content_1381960.htm

(Adopted at the 11th Meeting of the Standing Committee of the Tenth National People's Congress on August 28, 2004 and promulgated by Order No.18 of the President of the People's Republic of China on August 28, 2004)

Chapter I
General Provisions

Article 1

This Law is enacted in order to standardize acts of electronic signature, validate the legal effect of electronic signature, and safeguard the lawful rights and interests of the parties concerned.

Article 2

For the purposes of this Law, electronic signature means the data in electronic form contained in and attached to a data message to be used for identifying the identity of the signatory and for showing that the signatory recognizes what is in the message.

The data message as mentioned in this Law means the information generated, dispatched, received or stored by electronic, optical, magnetic or similar means.

Article 3

The parties concerned may agree to use or not to use electronic signature or data message in such documentations as contracts and other documents, receipts and vouchers in civil activities.

The legal effect of a document, with regard to which the parties concerned have agreed to use electronic signature or data message, shall not be denied only because the form of electronic signature or data message is adopted.

The provisions of the preceding paragraphs shall not be applicable to the following documents:

(1) documents relating to such personal relations as marriage, adoption and succession;
(2) documents relating to the transfer of the rights and interests residing in such real estate as land and houses;
(3) documents relating to termination of such public utility services as water supply, heat supply, gas supply and power supply; and
(4) other circumstances where electronic documentation is not applicable, as provided for by laws and administrative regulations.

Chapter II
Data Message

Article 4

A data message, which can give visible expression to the contents carried and can readily be picked up for reference, shall be deemed to be the written form which conforms to the requirements of laws and regulations.

Article 5

Data messages that meet the following conditions shall be deemed to satisfy the requirements for the form of the original copies as provided for by laws and regulations:

(1) messages that can give effective expression to the contents carried and can readily be picked up for reference; and
(2) messages that can unfailingly guarantee that the contents remain complete and unaltered from the time when they are finally generated. And the completeness of the data messages shall not be affected when endorsements are added to the data messages or when their forms are altered in the process of data interchange, storage and display.

Article 6

Data messages that meet the following conditions shall be deemed to satisfy the

requirements for document preservation as provided for by laws and regulations:

(1) messages that can give effective expression to the contents carried and can readily be picked up for reference;
(2) the format of the data messages is the same as the format when they are generated, dispatched or received, or although the format is not the same, the contents originally generated, dispatched or received can accurately be expressed; and
(3) messages the addressers and receivers of which and the time of their dispatch and receipt can be identified.

Article 7

No data messages to be used as evidence shall be rejected simply because they are generated, dispatched, received or stored by electronic, optical, magnetic or similar means.

Article 8

The following factors shall be taken into consideration when the truthfulness of data messages to be used as evidence is examined:

(1) the reliability of the methods used for generating, storing or transmitting the data messages;
(2) the reliability of the methods used for keeping the completeness of the contents;
(3) the reliability of the methods for distinguishing the addressers; and
(4) other relevant factors.

Article 9

Any of the following data messages shall be deemed to be dispatched by the addresser:

(1) the data message is dispatched with authorization of the addresser;
(2) the data message is dispatched automatically by the information system of the addresser; and
(3) verification of the data message made by the receiver in accordance with the method recognized by the addresser proves that the message is identical with the one dispatched.

If the parties concerned have agreed otherwise with regard to the matters specified in the preceding paragraph, such agreement shall be complied with.

Article 10

If confirmation of receipt of a data message is required pursuant to the provisions of laws and administrative regulations or the agreement reached between the parties concerned, such receipt shall be confirmed. When the addresser receives the confirmation of the receipt sent by the receiver, the data message shall be deemed to have been received.

Article 11

The time when a data message enters into a certain information system beyond the control of the addresser shall be deemed to be the time when the message is dispatched.

If a receiver designates a special system for receipt of a data message, the time when the message enters into the system as designated shall be deemed to be the time when the said message is received; and if no special system is designated, the first time when the data message enters into any systems of the receiver's shall be deemed to be the time when the message is received.

If the parties concerned have agreed otherwise on the time of dispatch or the time of receipt of data messages, such agreement shall be complied with.

Article 12

The principal business place of an addresser shall be the place of dispatch of data messages, and the principal business place of a receiver shall be the place of receipt of data messages. If there are no principal business places, their habitual residences shall be the places of dispatch or receipt.

If the parties concerned have agreed otherwise on the place of dispatch or the place of receipt of data messages, such agreement shall be complied with.

Chapter III
Electronic Signature and Certification

Article 13

If an electronic signature concurrently meets the following conditions, it shall be deemed as a reliable electronic signature:

(1) when the creation data of the electronic signature are used for electronic signature, it exclusively belongs to an electronic signatory;
(2) when the signature is entered, its creation data are controlled only by the electronic signatory;
(3) after the signature is entered, any alteration made to the electronic signature can be detected; and
(4) after the signature is entered, any alteration made to the contents and form of a data message can be detected.

The parties concerned may also choose to use the electronic signatures which meet the conditions of reliability they have agreed to.

Article 14

A reliable electronic signature shall have equal legal force with handwritten signature or the seal.

Article 15

An electronic signatory shall have the creation data of his electronic signature well preserved. When an electronic signatory learns that the creation data of his electronic signature have got lost or may have got lost, he shall make it known to all the parties concerned in time and terminate the use of such data.

Article 16

If an electronic signature needs to be verified by a third party, the electronic verification service established according to law shall provide such service.

Article 17

An electronic verification service shall meet the following conditions:

(1) having the professional technicians and managerial personnel suited for provision of electronic verification services;
(2) having the funds and business places suited for provision of electronic verification services;
(3) having the technology and equipment complying with the safety standards of the State;
(4) having the certificates for the use of the codes approved by the code control institution of the State; and
(5) other conditions prescribed by laws and administrative regulations.

Article 18

A person that intends to engage in electronic verification service shall make an application to the department in charge of the information industry under the State Council and submits the materials proving fulfilment of the conditions as specified by Article 17 of this Law. Upon receiving the application, the department in charge of the information industry under the State Council shall examine it according to law and consult with the department in charge of commerce and other relevant departments under the State Council, before making a decision on whether to grant or deny approval within 45 days from the date it receives the application. If it grants approval, it shall issue the license of electronic verification; and if it denies approval, it shall inform the applicant in writing of the fact and of the reasons why.

The applicant shall, upon the strength of the license of electronic verification, go through the formalities for enterprise registration at the administrative department for industry and commerce according to law.

The electronic verification service that has been qualified for verification shall, in accordance with the regulations of the department in charge of the information industry under the State Council, make public in the Internet such information as its name and the number of its license.

Article 19

The electronic verification service shall formulate and publish its rules for electronic verification, which are in conformity with the relevant regulations of the State and submit them to the department in charge of the information industry under the State Council for the record.

The rules for electronic verification shall include the matters such as the scope of liability, the norms for operation and the protective measures for information safety.

Article 20

When an electronic signatory applies to an electronic verification service for the certificate of his electronic signature, he shall provide truthful, complete and accurate information.

Upon receiving the application for certificate of the electronic signature, the electronic verification service shall check the identity of the applicant and examine the relevant materials.

Article 21

The certificate of an electronic signature issued by the electronic verification service shall be accurate and devoid of error, and the following items shall clearly be stated therein:

(1) the name of the electronic verification service;
(2) the name of the certificate holder;
(3) the serial number of the certificate;
(4) the term of validity for the certificate;
(5) the validation data of the electronic signature of the certificate holder;
(6) the electronic signature of the electronic verification service; and
(7) other items as prescribed by the department in charge of the information industry under the State Council.

Article 22

An electronic verification service shall guarantee that the items in the certificate of an electronic signature are complete and accurate within the term of its validity, and guarantee the party relying on the electronic signature the ability to prove or to know the items stated in the certificate of the electronic signature and other relevant matters.

Article 23

If an electronic verification service intends to suspend or terminate the service, it shall, 90 days prior to the suspension or termination of service, notify the parties concerned of how to get continued services and of other relevant matters.

If an electronic verification service intends to suspend or terminate the service, it shall report to the department in charge of the information industry under the State Council 60 days prior to the suspension or termination of service and shall make proper arrangements by negotiating with other electronic verification services on how to carry on its business.

If an electronic verification service fails to reach an agreement with other electronic verification services on matters of how to carry on its business, it shall apply to the department in charge of the information industry under the State Council for arranging other electronic verification services to carry on its business.

If the license of electronic verification of an electronic verification service is revoked according to law, its business shall be carried on in accordance with the regulations of the department in charge of the information industry under the State Council.

Article 24

An electronic verification service shall have the information relating to verification well preserved. The time limit for preservation of such information shall at least be five years after the certificate of the electronic signature ceases to be valid.

Article 25

The department in charge of the information industry under the State Council shall, in accordance with this Law, formulate the specific measures for administration of the electronic verification services and exercise supervision over the electronic verification services according to law.

Article 26

Upon examination and approval by the department in charge of the information industry under the State Council on the basis of relevant agreements or the principle of reciprocity, the certificates of electronic signatures issued by overseas electronic verification services outside of the territory of the People's Republic of China shall have equal legal force with the ones issued by the electronic verification services established in accordance with this Law.

Chapter IV
Legal Responsibility

Article 27

An electronic signatory who, having learnt that the creation data of his electronic signature have got lost or might have got lost, fails to notify in time the parties concerned of the fact and to terminate the use of the same, who fails to provide the electronic verification service with truthful, complete and accurate information, or who makes other errors, thus causing losses to the party relying on the electronic signature and to the electronic verification service, shall bear the responsibility for compensation.

Article 28

Where an electronic signatory or the party relying on the electronic signature suffers losses due to engaging in civil activities on the basis of the electronic signature verified by an electronic verification service, and if the electronic verification service fails to prove that it is free from fault, the service shall bear the responsibility for compensation.

Article 29

Where a person provides electronic verification services without permission, the department in charge of the information industry under the State Council shall order him to desist from the illegal act; the unlawful gains, if any, shall be confiscated; if such gains exceed RMB 300,000 yuan, a fine of not less than one time but not more than three times the unlawful gains shall be imposed; and if there are no unlawful gains or the amount of such gains is less than 300,000 yuan, a fine of not less than 100,000 yuan but not more than 300,000 yuan shall be imposed.

Article 30

Where an electronic verification service that intends to suspend or terminate electronic verification services fails to report to the department in charge of the information industry under the State Council 60 days prior to the suspension or termination of service, the said department shall impose a fine of not less than 10,000 yuan but not more than 50,000 yuan on the person who is directly in charge of the service.

Article 31

Where an electronic verification service fails to observe the rules for verification, fails to have the information relating to verification well preserved, or commits other illegal acts, the department in charge of the information industry under the State Council shall order it to rectify within a time limit; if it fails to comply at the expiration of the time limit, its electronic verification license shall be revoked, and the persons who are directly in charge of the service and the other persons who are directly responsible shall be prohibited from engaging in electronic verification services within the period of 10 years. If an electronic verification license is revoked, the fact shall be made known to the public and the administrative department for industry and commerce shall be informed of the same.

Article 32

Where a person counterfeits, copies or usurps the electronic signature of another person's, which constitutes a crime, his criminal responsibility shall be investigated according to law; and if losses are caused to another person, he shall bear civil responsibility according to law.

Article 33

Where a staff member of the department in charge of supervision and administration over

the electronic verification industry in accordance with this Law fails to perform his duties of granting administrative license and exercising supervision and administration according to law, he shall be given an administrative sanction according to law; and if a crime is constituted, he shall be investigated for the criminal responsibility according to law.

Chapter V
Supplementary Provisions

Article 34

The meanings of the following terms used in this Law are:

(1) the electronic signatory means a person who holds the creation data of an electronic signature and produces the electronic signature either in person or on behalf of the person he represents;
(2) the relying party on the electronic signature means the person who engages in relevant activities on the basis of his trust in the certificate of the electronic signature or the electronic signature;
(3) the certificate of the electronic signature means a data message or other electronic records that can prove the connection between the electronic signatory and the creation data of the electronic signature;
(4) the creation data of an electronic signature means such data as the characters and codes that are used in the course of the electronic signature and that reliably connects the electronic signature with the electronic signatory; and
(5) the validation data of an electronic signature means the data used for verifying the electronic signature, including the code, password, algorithm and public key.

Article 35

The State Council or the departments specified by the State Council may, in accordance with this Law, formulate specific measures for the use of the electronic signatures and data messages in administrative and other public activities.

Article 36

This Law shall go into effect as of April 1, 2005.