SOME PROVISIONS IN THE DRAFT LAW ON E-TRANSACTIONS (AMENDED)

PHUONG UYEN

The Law on E-Transactions 2005 (**LET 2005**), which took effect on March 1, 2006, is considered a frame law regulating technical and specific issues arising in the electronic environment. However, in the context of the industrial revolution 4.0 and the strong explosion of demand for e-transactions, especially during the Covid-19 pandemic, LET 2005 has revealed certain shortcomings and limitations. In order to meet the practical requirements of socio-economic development and ensure the consistency with relevant legal provisions, the Law on E-Transactions (amended) (**the Draft Law**) is being drafted by the Ministry of Information and Communication and is currently in the process of collecting public comments. In this month's Legal Newsletter, NHQuang&Associates would like to review some notable amendments and supplements of this Draft Law for clients' overview of the Draft's provisions that possibly affect enterprises' business operations.

Regulations on data messages

In order to ensure the legal validity, reliability and security of data messages, the Draft Law has amended and supplemented the provisions on legal validity of data messages as well as those related to sending and receiving data messages and e-certificates. Specifically:

(i) Supplementing the forms for creating and converting data messages. Accordingly, data messages can be created, self-generated in the transaction process or digitized from hard copies.

(ii) Setting hierarchy for legal validity of data messages. The reliability levels of data messages are ranged from low to high, including:

- Level 1: Data message without information about the sender or creator and it is impossible to verify, certify the integrity of the data message;
- Level 2: Data message without information about the sender or creator or with information about the sender or creator but it is not certified and the integrity of the data message is certified through at least one independent electronic means such as telephone, email;
- Level 3: Data message with certified information about the sender or creator and the integrity of the data message is certified through at least one independent electronic means such as telephone, email;
- Level 4: Data message with certified information about the sender or creator and the security of the data message is certified by secure electronic certification facility provided by licensed certification service provider or competent state agencies as prescribed by law.

(iii) Supplementing regulations on digital transformation, thereby replacing the paper-based storage of documents, vouchers, records, and materials with data message.

(iv) Supplementing regulations on the concept, legal validity and use of e-certificates. Accordingly, an e-certificate is understood as a data message issued by competent agency or organization, which recognizes or certifies the legal status, legal behavior, legal ownership and use rights of individuals, organizations or certifies that a vehicle, machine, equipment, product or service meets certain standards prescribed by law. The legal validity, effectiveness, usability or enforceability of an e-certificate shall not be rejected simply because of its electronic form. In addition, the Draft Law stipulates the conditions to ensure reliability when using and storing e-certificates as well as conditions for e-certificates to replace certificates, degrees, diplomas in print or vice versa.

While LET 2005 just addresses the legal validity of data messages to facilitate the transfer of traditional transactions to electronic environment without clarifying the regulations on secure data messages, the Draft Law has detailed the regulations, ensuring the integrity and non-repudiation of data messages, ensuring legal validity for enforcement, creating a basis for establishing secure e-transactions in the network environment.

Regulations on the legal validity of e-signatures

Regarding the legal validity of e-signatures, LET 2005 stipulates that an e-signature is legally valid when satisfying 2 conditions: (i) The method creating the e-signature permits to identify the signatory and indicate his/her approval of the data message contents; (ii) Such method is sufficiently reliable and appropriate for the purpose for which the data message is created and sent. This regulation aims to create a legal foundation for implementing e-transactions in the network environment; however, the Law does not specifically stipulate secure signatures, measures and standards to ensure secure e-signatures. In addition, the lack of regulations on the level of e-signatures, the legal validity of e-signatures by level, etc. has created a barrier in determining the legal validity of e-signatures for practical application, and also caused difficulty when there is any dispute over the transaction. The Draft Law has overcome the above issues by supplementing such provisions as:

- Regulations on secure e-signatures, use principles associated with the legal validity of e-signatures, accordingly, an e-signature will be legally valid if it satisfies the following conditions: (i) Permit to identify the signatory; (ii) Ensure that the data message content is not changed; (iii) Be created by secure electronic means, controlled only by the signatory at the time of signing; (iv) Be certified by secure e-signature certification service provider.
- Regulations on the State's responsibility in recognizing the legal validity of e-signatures and e-certificates; reclassifying organizations providing e-signature certification services into organizations providing secure e-signature certification services and providing specialized e-signature certification services (enclosed with regulations on conditions and eligibility certification for each organization).

Through the above contents, it can be seen that the Draft Law strictly regulates the legal validity of e-signatures, and also tightens the management of related issues. This is the basis to ensure efficient application and enforcement of e-signatures, a prerequisite for deploying secure e-transactions and digital transformation in the near future.

Regulations on e-contracts

The Draft Law recognizes the legal validity of e-contracts based on the reliability level of entities involving in e-contracts and contract conclusion process, including: (i) Transaction subjects (electronic transaction accounts); (ii) Contract data messages; (iii) Electronic documents attached to the contract (if any); (iv) Other entities associated with e-contracts and e-contracting process.

In addition, the Draft Law also stipulates in detail the principles of concluding and performing an e-contract, the stages of conclusion from the offer notice, offer, review, content confirmation to offer-reply, offer termination; stipulates model e-contracts to protect the interests of consumers; at the same time, stipulates that the model contract between users on the platforms must refer to the mediation/arbitration organizations providing authorized online mediation/arbitration.

In general, LET 2005 and the Draft Law both recognize that the legal validity of e-contracts cannot be denied just because the contract is presented in the form of a data message. However, the Draft Law stipulates more clearly the criteria for determining the legal validity of e-contracts as well as the process for e-contract conclusion in order to create a legal basis to ensure the implementation of secure, reliable, legally valid e-transactions in cyberspace as well as to encourage enterprises in choosing e-contracts for commercial acts as an alternative to other tradi-tional transaction methods.

Services of reliability certification and support for e-transactions

Services of reliability certification and support for e-transactions are a group of new regulations compared to LET 2005, detailed in Chapter VI of the Draft with 10 articles (From Article 40 to Article 50), whereby:

- Services of reliability certification in e-transactions (referred to as reliability certification services) are services performed by service providers through the network environment in order to verify and certify the trustworthiness of e-transactions including: (i) E-signature certification service; (ii) Timestamp certification service; (iii) Data message and e-certificate certification service; (iv) E-transaction, e-conclusion and e-contract certification services (Clause 1, Article 40 of the Draft Law).
- E-transaction support services are services performed by service providers through the network environment in order to support,

promote, and participate in the implementation of part or the whole of the e-transaction process (Clause 2, Article 40 of the Draft Law).
- Digital credit services are services performed by service providers that aim to assess the reliability of e-transaction systems and provide information on the reliability of subjects in e-transactions, including: (i) Credit rating service of e-transaction system; (ii) Digital credit rating information service (Clause 3, Article 40 of the Draft Law).

As we all know, in current e-transaction activities, reliability certification services are an important factor throughout the implementation of e-transactions. A provider of reliability certification service is an entity entrusted by the parties to perform activities related to certifying the reliability of related documents and operations during the e-transaction process. However, reliability certification services and related issues have not been regulated in LET 2005, leading to the lack of a legal framework governing e-transactions, affecting the assurance of the legal validity of e-transactions. Therefore, the Draft Law has added a new set of regulations on services of reliability certification to overcome technical weaknesses in the provisions of LET 2005 to make e-transaction activities more professional, in line with the practical requirements.

Safety, security, protection, confidentiality in electronic transactions

Besides inheriting the regulations on security, safety, protection and confidentiality in e-transactions in LET 2005, the Draft Law also amends and supplements the missing regulations related to safety, protection, confidentiality, and handling of requirements arising in the process of digital transformation, socio-economic development and e-transactions in the context of complicated cyber safety and cybersecurity, and also in compliance with the Law on Cyberinformation Security 2015 and the Law on Cybersecurity 2018. Accordingly, the Draft Law supplements the regulations on ensuring data security in e-transactions in Section 1 on data classification; responsibilities of the Ministry of Information and Communications for data security; responsibilities for data processing of organizations and individuals; responsibilities of organizations providing intermediary services for e-transactions; ensuring the security of cross-border transferred data.

In Section 2 on Cyberinformation security and Cybersecurity in e-transactions, the Draft Law supplements the regulations on securing e-transactions, accordingly, an e-transaction is secure when ensuring at minimum the following criteria: (i) Provision of counter authentication (customer or cardholder and merchant authentication); (ii) Secure payment and order information with appropriate encryption; (iii) Resistibility to modification of data messages; (iv) Interoperability and security assurance mechanisms. In addition, the Draft also supplements the regulations on state agencies' access and use of information in the digital environment to ensure the legal basis to protect information security for people and enterprises when most public administrative services are carried out on electronic portals according to the Government's digital transformation plan.

The assurance of safety and security in e-transactions, protection of electronic data messages and information confidentiality in e-transactions for enterprises is a crucial matter. In addition to the benefits from e-transactions like saving cost and time, there are also certain risks such as the risk of losing electronic data, forging information, signatures, etc. Therefore, enterprises need to understand the above regulations and develop solutions to prevent risks by using secure software, building a secure and organized electronic storage system, develop an implementation process related to e-transactions within the enterprises.

The current Draft Law has expanded the application scope of e-transactions to all activities of social life, from activities of state agencies to economic, social, civil, commercial, financial, banking activities, etc., and may continue to have other important modifications. Enterprises should pay attention to update information and follow up the drafting process of the Draft Law to ensure that their activities and policies comply with the provisions of law. We shall continue our updates once the Law on E-Transactions (amended) officially takes effect.