THE STATE PRESIDENT

ORDER No. 23/2005/L-CTN OF DECEMBER 9, 2005, ON LAW PROMULGATION

THE PRESIDENT OF THE SOCIALIST REPUBLIC OF VIETNAM

Pursuant to Article 103 and Article 106 of the 1992 Constitution of the Socialist Republic of Vietnam, which was amended and supplemented under Resolution No. 51/2001/QH10 of December 25, 2001, of the Xth National Assembly, the 10th session;

Pursuant to Article 91 of the Law on Organization of the National Assembly;

Pursuant to Article 50 of the Law on Promulgation of Legal Documents,

HEREBY PROMULGATES:

The Law on E-Transactions,

which was passed on November 29, 2005, by the XIth National Assembly at its 8th session.

President of the Socialist Republic of Vietnam
TRAN DUC LUONG

LAW ON E-TRANSACTIONS

(No. 51/2005/QH11)

Pursuant to the 1992 Constitution of the Socialist Republic of Vietnam, which was amended under Resolution 51/2001/QH10 of December 25, 2001, of the Xth National Assembly, the 10th session;

This Law provides for e-transactions.

Chapter I

GENERAL PROVISIONS

Article 1- Governing scope

This Law provides for e-transactions in the operations of state agencies; the civil, business, commercial and other sectors prescribed by law.

The provisions of this Law shall not apply to the grant of certificates of land use rights, house ownership right and immovable properties, inheritance documents, marriage certificates, divorce decisions, birth certificates, death certificates, bills of exchange and other valuable papers.

Article 2.- Subjects of application

This Law shall apply to agencies, organizations and individuals opting for transactions by electronic means.

Article 3.- Application of the Law on E-Transactions

In case of difference between the provisions of the Law on E-Transactions and other provisions of law on the same matter related to e-transactions, the provisions of the Law on E-Transactions shall apply.

Article 4.- Term interpretation

In this Law, the following terms are construed as follows:

1. *An e-certificate* means a data message issued by an e-signature certification service-providing organization in order to verify that the certified agency, organization or individual is the person having made the e-signature.

2. *Certification of an e-signature* means verification that the certified agency, organization or individual is the person having made the e-signature.

3. *Electronic signing program* means a computer program established to operate independently or through equipment, information system, other computer programs in order to create an e-signature typical for the person who signs data messages.

4. *Database* means a compilation of data arranged and organized for access, exploitation, management and updating of information through electronic means.

5. *Data* mean information in form of symbol, script, numeral, image, sound or the like.

6. An e- transaction means a transaction implemented by electronic means

7. An automatic e-transaction means an e-transaction which is automatically performed in part or in whole through a pre-established information system.

8. *An information system* means a system established for sending, receiving, storing, displaying or another processing with respect to data messages.

9. *An intermediary* means an agency, organization or individual, that represents another agency, organization or individual to send, receive or store a data message or to provide other services relating to such data message.

10. *An electronic means* is a means that operates based on electric, electronic, digital, magnetic, wireless, optical, electro-magnetic technologies or similar technologies.

11. *A security control process* is a process used to verify sources of data messages, e-signatures; to discover changes or mistakes appearing in the content of a data message in the process of transmission, receipt and storage.

12. *A data message* means information created, transmitted, received and stored by electronic means.

13. *An e-signature certification service-providing organization* means an organization carrying out e-signature certification activities in accordance with the provisions of law.

14. *An online service-providing organization* means an organization providing transmission line infrastructure and other relevant services to carry out e-transactions. Online service-providing organizations include Internet access providers, Internet service providers and online service providers.

15. *Electronic data interchange (EDI)* means the transfer of information from one computer to another by electronic means in accordance with an agreed standard on information structure.

Article 5.- General principles in e-transactions

1. To voluntarily select electronic means for transactions.

2. To mutually agree on the selection of type of technology for e-transactions.

3. No technology shall be considered the sole [technology] in e-transactions.

4. To ensure equality and security in e-transactions.

5. To protect lawful rights and interests of agencies, organizations, individuals, interests of the State and public interests.

6. E-transactions of State agencies must comply with the principles stipulated in Article 40 of this Law.

Article 6.- Policies on development and application of e-transactions

1. To give priority to the development of technological infrastructure and training of human resources related to e-transactions.

2. To encourage agencies, organizations and individuals to invest in and apply e-transactions in accordance with the provisions of this Law.

3. To support e-transactions in public services.

4. To step up the implementation of e-commerce, transactions by electronic means and computerization of the state bodies' operations.

Article 7.- Contents of the state management of e-transactions

1. To issue and organize the implementation of strategies, plannings, plans and policies for developing and applying e-transactions in the socio-economic, defence and security domains.

2. To promulgate, propagate and implement legal documents on e-transactions.

3. To promulgate and recognize e-transaction standards.

4. To manage organizations providing services related to e-transactions.

5. To manage the development of technological infrastructure for e-transaction activities.

6. To organize and manage the training, fostering and building of the contingent of personnel and experts in the e-transaction domain.

7. To inspect and supervise the implementation of law on e-transactions; to settle complaints and denunciations, to handle acts of violating law on e-transactions.

8. To manage and carry out activities of international cooperation on e-transactions.

Article 8.- Responsibilities of the state management of e-transactions

1. The Government shall exercise the uniform management over e-transaction activities.

2. The Ministry of Post and Telematics shall take responsibility before the Government, assuming the prime responsibility for, and coordinating with relevant ministries and branches in, exercising the state management of e-transaction activities.

3. Ministries and ministerial-level agencies shall, within the ambit of their tasks and powers, have to exercise the state management over e-transaction activities.

4. People's Committees of provinces or centrally-run cities shall, within the ambit of their tasks and power, exercise the state management of e-transaction activities in their respective localities.

Article 9.- Prohibited acts in e-transactions

1. Obstructing the selection of the use of e-transactions.

2. Illegally obstructing or preventing the process of transmitting, sending and receiving data messages.

3. Illegally modifying, deleting, cancelling, counterfeiting, copying, disclosing, displaying or moving part or whole of a data massage.

4. Creating or disseminating software programs that trouble, change or destroy operating system or committing other acts to destroy the technological infrastructure on e-transactions.

5. Creating data messages in order to commit illegal acts.

6. Tricking, wrongly identifying, appropriating or illegal using e-signatures of others.

Chapter II

DATA MESSAGE

Section 1. LEGAL VALIDITY OF DATA MESSAGES

Article 10.- Formats of data message

A data message may be shown in the form of electronic data interchange, electronic documents, e-mails, telegrams, telegraphs, facsimiles and other similar forms.

Article 11.- Legal validity of data message

Information in data messages cannot have its legal validity disclaimed for the sole reason that it is expressed in the form of data messages.

Article 12.- Data messages being as valid as documents

Where the law requires information to be in writing, a data message shall be considered having met this condition if the information contained therein is accessible and usable for reference when necessary.

Article 13.- Data message being as valid as original copy

A data message shall be as valid as an original copy when satisfying the following conditions:

1. The contents of the data message are kept intact since its first origination in the form of a complete data message.

The contents of a data message are considered intact when they remain unchanged, except for changes in their appearance, which arise in the process of sending, storage or display of the data message.

2. The contents of the data message are accessible and usable in its integrity for reference when necessary.

Article 14.- Data message being as valid as evidence

1. A data message cannot be disclaimed in terms of its validity as evidence for the sole reason that it is a data message.

2. The validity as evidence of a data message shall be determined based on the reliability of the manner in which the data message was generated, stored or communicated; the manner to ensure and maintain the integrity of the data message; the manner in which its originator was identified, and on other relevant factors.

Article 15.- Storage of data message

1. In cases where the law requires records, files or information to be stored, such records, files or information can be stored in the form of data messages when the following conditions are satisfied:

a/ The information in the data message is accessible and usable for reference when necessary;

b/ The contents of such data message are stored in the very format in which it was originated, sent or received, or in a format which can be demonstrated to represent accurately its contents;

c/ Such data message is stored in a manner to enable the identification of its origin, destination, and the date and time when it was sent or received.

2. Contents and time limit for storage of data message shall comply with the provisions of law on storage.

Section 2. SENDING AND RECEIPT OF DATA MESSAGES

Article 16.- Originator of a data message

1. The originator of a data message shall be an agency, organization or individual that creates or sends the data message before such message is stored, excluding any intermediary transmitting the data message.

2. Where parties to a transaction do not agree otherwise, the identification of the originator of a data message shall be as follows:

a/ A data message is considered as that of the originator if it is sent by the originator or by an information system established and designated by the originator to operate automatically;

b/ The recipient may consider a data message as being that of the originator if [the recipient] has applied the verification methods approved by the originator and such methods give the result that such data message is of the originator;

c/ As from the time the recipient becomes aware of technical errors in the transmission of a data message or has applied error-detecting methods approved by the originator, the provisions of Points a and b of this Clause shall not apply.

3. The originator shall take responsibility before law for the contents of the data message he/she/it has originated.

Article 17.- Time and place of sending a data message

Unless otherwise agreed upon by the parties to a transaction, the time and place of sending a data message is provided for as follows:

1. The time of sending a data message is the point of time when such data message enters an information system outside the control of the originator;

2. Place of sending a data message is the headquarters of the originator if the originator is an agency or organization or the permanent residence of the originator if the originator is an individual. If the originator has more than one headquarters, the place of sending the data message is the one which has the closest relationship with the transaction.

Article 18.- Receipt of a data message

1. The recipient of a data message is the person who is designated to receive the data message from its originator but does not mean any intermediary transmitting such data message.

2. Unless otherwise agreed upon by the parties to the transaction, the receipt of a data message is provided for as follows:

a/ The recipient of a data message is deemed in receipt of such message if the message is entered into an information system designated by him/her/it and accessible;

b/ The recipient may consider each data message an independent one unless such message is a copy of another data message and the recipient knows or ought to know that it is a copy;

c/ Where the originator has required or agreed with the recipient before or during the sending of a data message that the recipient must send an acknowledgement of the receipt of such message, the recipient must comply with such request or agreement;

d/ Where the originator, before or during the sending of a data message, has stated that such message will be valid only when he/she/it receives an acknowledgement, such data message shall be considered having not been sent till the originator receives a written acknowledgement of the receipt of such message from the recipient;

e/ Where the orginator has already sent a data message without stating that the recipient must send an acknowledgement and has not yet received the acknowledgement, the originator may notify the recipient that no acknowledgement has been received and set a

reasonable duration for the recipient to send the acknowledgement. If the originator still fails to receive any acknowledgement within the specified duration, he/she/it may treat the data message as though it had never been sent.

Article 19.- Time and place of receiving a data message

Unless otherwise agreed upon by the parties to the transaction, the time and place of receiving a data message are provided for as follows:

1. If the recipient has designated an information system for receiving a data message, the mesage-receiving time shall be the time when the data message enters the designated information system; if the recipient has not designated a specific information system for receiving the data message, the mesage-receiving time shall be the time when the data message enters any information system of the recipient.

2. The place of receiving a data message shall be the headquarters of the recipient if the recipient is an organization or the permanent residence of the recipient if the recipient is an individual. If the recipient has more than one headquarters, the place of receiving the data message shall be the headquarters, which has the closest relationship with the transaction.

Article 20.- Automatic sending and receipt of data messages

If the orginator or the recipient has designated one or several information systems for the purpose of automatic sending or receipt of data messages, the provisions of Articles 16, 17, 18 and 19 of this Law shall apply.

Chapter III

E-SIGNATURES AND CERTIFICATION OF E-SIGNATURES

Section 1. LEGAL VALIDITY OF E-SIGNATURES

Article 21.- E-signatures

1. An e-signature is established in the form of words, letters, numerals, symbols, sounds or other forms by electronic means, logically attached or associated with a data message and capable of certifying the person who has signed it as well as the approval of such person to the content of the signed data message.

2. An e-signature shall be considered secured if it satisfies the conditions stipulated in Clause 1, Article 22 of this Law.

3. E-signatures may be certified by e-signature certification service providing organizations.

Article 22.- Conditions to ensure security of e-signatures

1. An e-signature is considered secured if it is verified by a security verifying process agreed upon by transacting parties and satisfying the following conditions:

a/ E-signature creation data are attached only to the signatory in the context that such data are used;

b/ E-signature creation data are under the control of only the signatory at the time of signing;

c/ All changes to the e-signature after the time of signing are detectable;

d/ All changes to the contents of the data message after the time of signing are detectable.

2. E-signatures certified by e-signature certification service-providing organizations shall be considered having satisfied the security conditions mentioned in Clause 1 of this Article.

Article 23.- Principles of using e-signatures

1. Unless otherwise provided for by law, the parties to a transaction have rights to reach agreement:

a/ To use or not to use e-signatures to sign data message in the transaction process; b/ To use or not to use the certified e-signature;

c/ To select an e-signature certification service-providing organization in cases where there is an agreement on the use of the certified e-signature.

2. E-signatures of state agencies must certified by e-signature certification service providing organizations defined by competent state agencies.

Article 24.- Legal validity of e-signatures

1. Where the law requires a document to be signed, such requirement with respect to a data message shall be considered having been met if an e-signature used for signing such data message satisfies the following conditions:

a/ The method of creating the e-signature permits to identify the signatory and to indicate his/her approval of the contents of the data message;

b/ Such method is sufficiently reliable and appropriate to the purpose for which the data message was originated and sent.

2. Where the law requires a document to be stamped with seal of the concerned agency or organization, such requirement with respect to a data message shall be considered having been met if the data message has an e-signature of the agency or organization that satisfies the conditions stipulated in Clause 1, Article 22 of this Law and the e-signature is certified.

3. The Government shall specify the management and use of e-signatures by agencies and organizations.

Article 25.- Obligations of the signatory of an e-signature

1. A signatory of an e-signature or his/her legal representative is the person who controls the electronic signing program and uses such equipment to certify his/her will regarding the signed data message.

2. A signatory of an e-signature shall have the following obligations:

a/ To take measures to avoid unauthorized use of his/her e-signature-creating data;

b/ To promptly use appropriate means to notify parties that accept the e-signature and the e-signature certification service-providing organization in case the e-signature is certified, when discovering that the e-signature may not be under his/her control;

c/ To apply necessary measures to ensure the accuracy and integrity of information included in the e-certificate in case such certificate is used to certify the e-signature.

3. A signatory shall take responsibility before law for all consequences of his/her failure to comply with the provisions of Clause 2 of this Article.

Article 26.- Obligations of the party accepting e-signatures

1. A party accepting e-signatures is the one that has implemented the contents in the received data messages based on the reliability of such e-signatures and e-certificates of the sender.

2. A party accepting e-signatures shall have the following obligations:

a/ To take necessary measures to verify the reliability of an e-signature before accepting it;

b/ To take necessary measures to verify legal validity of an e-certificate and any limitation with respect to the e-certificate in case such e-certificate is used to certify an e-signature.

3. The party accepting e-signatures shall take responsibility before law for consequences of non-compliance with the provisions of Clause 2 of this Article.

Article 27.- Recognition of foreign e-signatures and e-certificates

1. The Government recognizes the legal validity of foreign e-signatures and e-certificates if such e-signatures or e-certificates have the same level of reliability as those provided for by law. The determination of the reliability of foreign e-signatures and e-certificates must be based on recognized international standards, on treaties to which the Socialist Republic of Vietnam is a contracting party and other relevant factors.

2. The Government shall specify the recognition of foreign e-signatures and e-certificates.

Section 2. E-SIGNATURE CERTIFICATION SERVICES

Article 28.- E-signature certification service activities

1**.** Issuing**,** extending, suspending, restoring and revoking e-certificates.

2. Providing necessary information to assist the certification of e-signatures of persons who sign data messages.

3. Providing other services related to e-signatures and e-signature certification in accordance with the provisions of law.

Article 29.- Contents of an e-certificate

1. Information on the e-signature certification service-providing organization.

2. Information on the agency, organization or individual to whom the e-certificate is issued.

3. The identification number of the e-certificate.

4. The valid term of the e-certificate.

5. The data for examining the e-signature of the person who is granted the e-certificate.

6. The e-signature of e-signature certification service-providing organization.

7. Limitations on the purpose or scope of using the e-certificate.

8. Limitations on legal liabilities of the e-signature certification service-providing organization.

9. Other contents as provided for by the Government.

Article 30.- E-signature certification service-providing organizations

1. E-signature certification service-providing organizations include public e-signature certification service-providing organizations and specialized e-signature certification service-providing organizations which are licensed to carry out e-signature certification activities in accordance with the provisions of law.

2. A public e-signature certification service-providing organization is an organization providing e-signature certifications services to agencies, organizations or individuals for use in public activities. Activities of providing public e-signature certification services are conditional business activities as provided for by law.

3. A specialized e-signature certification service-providing organization is an organization providing e-signature certification services to agencies, organizations or individuals for use in specialized activities or domains. Activities of providing specialized e-certification services must be registered with state management bodies in charge of e-signature certification services.

4. The Government shall specify the establishment, organization, business registration, operation and mutual recognition of e-signature certification service-providing organizations defined in Clauses 2 and 3 of this Article.

Article 31.- Rights and obligations of e-signature certification service- providing organizations

1. E-signature certification service-providing organizations shall have the following rights and obligations:

a/ To carry out the e-signature certification service activities specified in Article 28 of this Law;

b/ To comply with the provisions of law on e-signature certification service-providing organizations;

c/ To use reliable technical equipment, processes and resources to perform their tasks;

d/ To guarantee the accuracy and integrity of substantial contents of e-certificates they have issued;

e/ To publicize information on e-certificates, which have been issued, extended, suspended, restored or revoked;

f/ To provide appropriate facilities to enable the e-signature-accepting parties and competent state agencies to rely on e-certificates to ascertain the origin of data messages and e-signatures;

g/ To notify the relevant parties of all incidents, which affect the certification of e-signatures.

h/ To publicize and notify the e-certificate grantees, and relevant management agencies of the suspension or termination of their operation within 90 days prior thereto.

i/ To archive information related to e-certificates they have issued for at least five years after such e-certificates become invalid.

j/ Other obligations as provided by law.

2. The Government shall specify the rights and obligations of e-signature certification service-providing organizations defined in Clause 1 of this Article.

Section 3. MANAGEMENT OF E-SIGNATURE CERTIFICATION SERVICES

Article 32.- Conditions for providing e-signature certification services

1. E-signature certification service-providing organizations must fully meet the following conditions:

a/ Having adequate professional technical and managerial staff to provide e-signature certification services.

b/ Having adequate technical means and equipment suitable to national security and safety standards;

c/ Registering the provision of e-signature certification services with the state management bodies.

2. The Government shall specify the following contents:

a/ Order and procedures for registration of e-signature certification service- providing activities.

b/ Technical standards, processes, human resources and other conditions necessary for e-signature certification service-providing activities.

c/ Contents and forms of e-certificates.

d/ Procedures for issuance, extension, suspension, restoration and revocation of e-certificates.

e/ The storage and disclosure of information related to e-certificates issued by e-certification service-providing organizations.

f/ Conditions and procedures for foreign e-signature certification service-providing organizations to provide e-signature certification services in Vietnam.

g/ Other contents necessary for e-signature certification service-providing activities.

Chapter IV

ENTRY INTO AND EXECUTION OF E-CONTRACTS

Article 33.- E-contracts

E-contracts mean contracts established in the form of data messages provided for in this Law.

Article 34.- Recognition of legal validity of e-contracts

The legal validity of an e-contract cannot be disclaimed for the sole reason that it is expressed as a data message.

Article 35.- Principles of entry into and execution of e-contracts

1. Participating parties shall have the right to reach agreement on the use of electronic means in the entry into and execution of contracts.

2. The entry into and execution of an e-contract shall comply with the provisions of this Law and law on contracts.

3. When entering into and executing e-contracts, the parties shall have the right to reach agreement on technical requirements, certification, conditions to ensure integrity and confidentiality related to such e-contracts.

Article 36.- Entry into e-contracts

1. Entry into e-contracts means the use of data messages to execute part or whole of transactions in the process of entering into contracts.

2. In the process of entering into contracts, unless otherwise agreed upon by concerned parties, an offer to enter into a contract and acceptance of the offer to enter into the contract may be carried out through data messages.

Article 37.- Receipt, sending, time, location of sending or receiving data messages in entering into and execution of e-contracts

The receipt, sending, time, location of sending or receiving data messages in entering into and execution of e-contracts shall be comply with Articles 17, 18, 19 and 20 of this Law.

Article 38.- Legal validity of a notice in entry into and execution of e-contracts

In the process of entering into and execution of an e-contract, a notice in the form of a data message shall be legally valid as a notice in another traditional form.

Chapter V

E-TRANSACTIONS OF STATE AGENCIES

Article 39.- Types of e-transactions of state agencies

1. E-transactions within a state agency;

2. E-transactions among different state agencies;

3. E-transactions between state agencies and other agencies, organizations and individuals.

Article 40.- Principles for conducting e-transactions of state agencies

1. Principles are provided for in Clauses 3, 4 and 5 of Article 5 of this Law.

2. E-transactions of state agencies must comply the provisions of this Law and relevant provisions of law.

3. A state agency shall, within its tasks and powers, take initiative in carrying out a part or all of transactions within it or with other state agencies by electronic means.

4. Based on socio-economic development conditions and their specific situations, state agencies shall determine a rational roadmap for the use of electronic means in the transaction types stipulated in Article 39 of this Law

5. Agencies, organizations and individuals shall have the right to select modes of transaction with state agencies if such state agencies concurrently accept transactions both in traditional forms and by electronic means, unless otherwise provided for by law.

6. When conducting e-transactions, state agencies must specify the following:

a/ Formats and forms of data messages;

b/ Types of e-signature, certification of e-signatures, for transactions requiring e-signatures or certification of e-signatures;

c/ Processes to ensure the integrity, security and confidentiality of e-transactions.

7. The provision of public services by state agencies in electronic forms shall be based on their respective regulations which, however, must not be contrary to the provisions of this Law and relevant provisions of law.

Article 41.- Security, confidentiality and storage of electronic information in state agencies

1. Periodically examining and ensuring security of electronic data systems of their respective agencies in e-transaction process.

2. Ensuring confidentiality of information related to e-transactions; not using information for other purposes contrary to the regulations on the use of such information; not disclosing information to a third party under the provisions of law.

3. Ensuring the integrity of data messages in e-transactions they conduct; ensuring security in operation of their computer networks;

4. Creating databases of corresponding transactions, ensuring information security and having standby systems to recover information in case of errors of the electronic information system.

5. Ensuring security, confidentiality and storage of information in accordance with the provisions of this Law and other relevant provisions of law.

Article 42.- Responsibilities of state agencies in case of errors of e-information systems

1. Where the e-information system of a state agency has errors, failing to ensure the security of data messages, such agency shall have to immediately notify the users thereof and take necessary measures to correct the errors.

2. State agencies shall take responsibility before the law for failure to comply with the provisions of Clause 1 of this Article.

Article 43.- Responsibilities of agencies, organizations and individuals in e-transactions with state agencies

Agencies, organizations and individuals, when conducting e-transactions with state agencies, shall comply with the provisions of this Law, the regulations on e-transactions, issued by competent state agencies and other relevant provisions of law.

Chapter VI

SECURITY, SAFETY, PROTECTION, CONFIDENTIALITY IN E-TRANSACTIONS

Article 44.- Ensuring security and safety in e-transactions

1. Agencies, organizations and individuals shall have the right to select measures to ensure security and safety in accordance with the provisions of law when conducting e-transactions.

2. Agencies, organizations and individuals conducting e-transactions must take necessary measures to ensure smooth operations of information systems under their control; if causing technical errors to such information systems which cause damage to other agencies, organizations and/or individuals, they shall be handled in accordance with the provisions of law.

3. Agencies, organizations and individuals must not take any action that prevents or adversely affects the protection of security and safety in e-transactions.

Article 45.- Protection of data messages

Agencies, organizations and individuals must not take any action that adversely affects the integrity of data messages of other agencies, organizations and/or individuals.

Article 46.- Information confidentiality in e-transactions

1. Agencies, organizations and individuals shall have the right to select security measures in accordance with the provisions of the law when conducting e-transactions.

2. Agencies, organizations and individuals must not use, provide or disclose information on private and personal affairs or information of other agencies, organizations and/or individuals which is accessible by them or under their control in e-transactions without the latter's consents, unless otherwise provided for by law.

Article 47.- Responsibility of online service-providing organizations

1. Online service-providing organizations shall have to co-coordinate with concerned agencies in elaborating management regulations and adopting technical measures to prevent and stop the use of their network services for dissemination of data messages which are against the cultural traditions, national ethics, or prejudicial to the national security, public order and safety or violate other provisions of law.

2. Online service-providing organizations shall take responsibility before law for delayed removal of data messages defined in Clause 1 of this Article, when they have received notices from competent state agencies.

Article 48.- Responsibilities of agencies, organizations and individuals upon the request of competent state agencies

1. When requested by competent state agencies, agencies, organizations and/or individuals shall have the following responsibilities:

a/ To store a particular data message, including the transfer of data to another computer system or another storage place;

b/ To maintain the integrity of a particular data message;

c/ To present or provide a particular data message, including its password and other encryption methods which they have or control;

d/ To present or provide information on the user of services in cases where the requested agencies, organizations or individuals are service providers controlling such information;

e/ Other responsibilities provided for by law.

2. Competent state agencies shall take responsibility before law for their requests.

Article 49.- Rights and responsibilities of state agencies

1. Competent state agencies shall have the following rights:

a/ To search or access part or all of a computer system and data messages in such system;

b/ To seize part or all of the computer system;

c/ To copy and store copies of data messages;

d/ To prevent access to a computer system;

e/ Other rights provided for by law.

2. When exercising the rights stipulated in Clause 1 of this Article, competent state agencies shall take responsibility before law for their decisions.

Chapter VII

DISPUTE SETTLEMENT AND VIOLATION HANDLING

Article 50.- Handling of violations of law on e-transactions

1. Any person violating law on e-transactions shall, depending on the nature and seriousness of their violations, be disciplined, administratively sactioned or examined for penal liabilities and, if causing damage, pay compensation under the provisions of law.

2. Agencies or organizations that commit acts of violating law on e-transactions shall, depending on the nature and seriousness of their violations, be administratively sanctioned, suspended from operation, and if causing damage, pay compensation therefor under the provisions of law.

Article 51.- Disputes in e-transactions

Disputes in e-transactions are disputes arising in the course of transaction by electronic means.

Article 52.- Settlement of disputes in e-transactions

1. The State encourages the disputing parties in e-transactions to settle disputes by themselves through concilliation.

2. Where the parties cannot resolve their disputes, the competence, order and procedures for the settlement of disputes over e-transactions shall comply with the provisions of law.

Chapter VIII

IMPLEMENTATION PROVISIONS

Article 53.- Effect

This Law shall take effect as from March 1, 2006.

Article 54.- Implementation guidance

The Government shall detail and guide the implementation of this Law.

This Law was passed on November 29, 2005, by the XIth National Assembly of the Socialist Republic of Vietnam at its 8th session.

Chairman of the National Assembly
NGUYEN VAN AN