2ND DRAFT
DECREE
PROVIDING DETAILED REGULATIONS ON A NUMBER OF ARTICLES OF THE LAW ON CYBERSECURITY

31 October 2018

CONTENTS

GOVERNMENT

SOCIALIST REPUBLIC OF VIETNAM

Independence - Freedom - Happiness

No. /2018/ND-CP

Ha Noi, 2018

2nd Draft dated 31 October 2018

DECREE
PROVIDING DETAILED REGULATIONS ON THE LAW ON CYBERSECURITY

Pursuant to the *Law on Organization of the Government* dated 19 June 2015;

Pursuant to the *Law on National Security* dated 3 December 2014;

Pursuant to the *Law on Cybersecurity* dated 12 June 2018;

On the proposal of the Minister of Public Security;

The Government hereby issues this Decree providing detailed regulations on a number of articles of the *Law on Cybersecurity*.

CHAPTER 1

General Provisions

Article 1 *Governing scope*

This Decree provides detailed regulations on articles 10.4, 12.5, 23.1(d), 24.7, 26.2(b), 26.4 and 36.5 of the *Law on Cybersecurity*.

Article 2 *Interpretation of terms*

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

1 *Enterprise providing services on telecom networks and on the Internet and value added services in cyberspace in Vietnam* means a domestic or foreign enterprise operating in accordance with the law of Vietnam or international law and providing the services prescribed in article 24 of this Decree.

2 *Administrator of an information system critical for national security* means an agency, organization or individual authorized/competent to directly manage such system.

CHAPTER 2

Formulation of the List of and Mechanisms for Coordination and Conditions for Protection of Information Systems Critical for National Security

Section 1

Formulation of the List of Information Systems Critical for National Security

Article 3 *Bases for establishing information systems critical for national security [critical information systems]*

Critical information systems in various sectors are prescribed in article 10.2 of the *Law on Cybersecurity* and when subject to an incident [breakdown], infiltration, hijacking of operational control, distortion, interruption, stoppage, paralysis, attack or destruction, will cause one of the following consequences:

1 Directly impacting on the existence of the regime and the State of the Socialist Republic of Vietnam.

2 Causing serious damage to national defence and security; weakening the ability to defend and protect the Homeland.

3 Becoming a means of information and propaganda against State administration and for overthrowing the regime.

4 Causing particularly serious consequences to the national economy.

5 Causing disaster to human life and the ecological environment.

6 Seriously affecting infrastructure of the national cyberspace.

7 Seriously affecting operations of construction works at level I and at the special level as delegated by the law on construction.

8 Seriously affecting activities of researching and formulating guidelines and policies classified as State secret.

9 Seriously affecting the direct instruction and administration by Party and State agencies at the central level.

Article 4 *Preparation of application file requesting to include an information system on the list of critical information systems*

1 Pursuant to article 3 of this Decree, ministers, heads of ministerial equivalent and Government agencies, chairmen of people's committees of provinces and cities under central authority and ["*provincial people's committees*"] political organizations at the central level are responsible to review and check against the bases for establishing critical information systems, prepare application files and request to include information systems under their management on the list of critical information systems.

Where necessary, the Cybersecurity Task Force [CTF] shall review information systems having bases for establishment in conformity with article 3 of this Decree and request administrators of critical information systems to prepare application files requesting to include information systems under their management on the list of critical information systems.

2 The application file requesting to include an information system on the list of critical information systems comprises:

(a) Official letter requesting to include the information system on the list of critical information systems, which contains the following contents: necessity of including the information system on the list, objectives, and requirements on protection; and conformity with the bases for establishment [of critical information systems];

(b) Documents and data proving conformity with the bases for establishing critical information systems.

Article 5 *Evaluation of application file requesting to include an information system on the list of critical information systems*

1 The CTF under the Ministry of Public Security [MPS] shall review and provide guidelines for preparing application files requesting to include information systems on the list of critical information systems, and receive and evaluate same, except for the provision in clause 2 of this article.

2 The CTF under the Ministry of Defence [MOD] shall provide guidelines for preparing application files requesting to include military information systems on the list of critical information systems, and review and evaluate same.

3 In necessary cases, the Minister of Public Security or the Minister of Defence shall make a decision establishing a council to evaluate application files requesting to include information systems on the list of critical information systems.

4 The CTF shall, within sixty (60) days from the date of receipt of a complete and valid application file requesting to include an information system on the list of critical information systems, make a proposal to the Minister of Public Security or the Minister of Defence for submission to the Prime Minister for his decision. The Minister of Public Security or the Minister of Defence shall decide to extend such time-limit if required.

Where necessary, the CTF shall conduct an actual survey to evaluate such request for including the information system on the list of critical information systems.

5 The applicant is responsible to coordinate with the CTF and facilitate the evaluation conducted by the CTF.

6 The Minister of Public Security or the Minister of Defence shall make a submission to the Prime Minister for promulgating and amending the list of critical information systems.

Article 6 *Removal of information systems from the list of critical information systems*

1 Every year, ministers, heads of ministerial equivalent and Government agencies, chairmen of provincial people's committees, and political organizations at the central level are responsible to review and identify information systems which no longer satisfy the bases stipulated in article 3 of this Decree and prepare application files requesting to remove such information systems from the list of critical information systems.

2 The application file requesting to remove an information system from the list of critical information systems comprises:

(a) Official letter requesting to remove the information system from the list, which contains the following basic contents: reasons and necessity for removal;

(b) Other documents and data relating to such request.

3 The sequence, procedures and authority to consider and make a decision removing an information system from the list of critical information systems shall comply with the provisions on sequence, procedures and authority to consider and make a decision including an information system on such list.

Section 2

Coordination in Evaluating, Inspecting and Supervising Information Systems Included in both the List of Critical Information Systems and the List of National Important Information Systems

Article 7 *Principles for coordination*

1 Comply with the *Law on Cybersecurity* and relevant laws.

2 Ensure proper performance of functions, duties and powers by each agency.

3 [Coordinate] actively, regularly, closely and promptly.

4 Ensure normal operation of critical information systems.

5 Coordination in evaluation, inspection and supervision applies to information systems included in both the list of national important information systems and the list of critical information systems.

With respect to other critical information systems not included on the list of critical information systems, the law on cybersecurity protection shall apply.[1]

Article 8 *Methods of coordination*

1 Direct communication, sending of official letters, and written notices.

2 Organization of inter-branch meetings.

3 Establishment of inter-branch working teams.

4 Other forms.

Article 9 *Coordination in inspecting information systems included on both the list of national important information systems and the list of critical information systems*

1 The CTF under the MPS shall preside over coordinating with the State administrative agency for information safety under the Ministry of Information and Communications [MOIC] and relevant agencies and organizations in inspecting cybersecurity and network information safety with respect to information systems included on both the list of national important information systems and the list of critical information systems, except for the provision in clause 2 of this article.

2 The CTF under the MOD shall preside over coordination in inspecting cybersecurity and network information safety with respect to military information systems included on the list of critical information systems.

3 Inspection results shall be used for servicing the work of protecting cybersecurity and network information safety.

Article 10 *Coordination in supervising information systems included on both the list of national important information systems and the list of critical information systems*

1 The CTF shall supervise and be responsible for the sharing of data from basic observation equipment for common use by competent agencies for the purpose of protecting cybersecurity and network information safety.

2 The administrator of a critical information system shall arrange a site and technical conditions, and set up and connect the supervisory system and/or equipment of the CTF to the information system managed by him/her with a view to detecting and providing early warning of the possibility of a loss of cybersecurity.

3 Where there is already a competent agency conducting supervision, data from basic observation equipment shall be shared with the CTF for common use for the purpose of protecting cybersecurity and network information safety.

Article 11 *Coordination in evaluating information systems included on both the list of national important information systems and the list of critical information systems*

[1] Allens footnote: This is the literal translation here.

1 When an information system is established, expanded or upgraded, the administrator sends an application file requesting evaluation of the plan on ensuring network information system to both the CTF under the MPS and the State administrative agency for information safety under the MOIC.

2 The CTF under the MPS shall preside over coordinating with the State administrative agency for information safety under the MOIC and relevant agencies and organizations in evaluating cybersecurity; and evaluating plans on ensuring network information safety when establishing, expanding or upgrading information systems included on both the list of national important information systems and the list of critical information systems.

Section 3

Cybersecurity Conditions Applicable to Critical Information Systems

Article 12 *Conditions on regulations, procedures and plans on protection of cybersecurity of critical information systems*

1 The administrator of a critical information system shall formulate regulations, procedures and plans on protection of cybersecurity of the critical information system managed by him/her on the basis of the regulations on protection of cybersecurity, protection of State secrets, technical regulations and standards on network information safety, and other relevant specialized technical standards.

2 The regulations, procedures and plans on protection of cybersecurity must specify the following contents: information system and important information for which protection is required to be prioritized; managerial, technical and professional procedures for using, and protecting cybersecurity of, data and technical infrastructure; conditions on personnel, especially personnel administering the network, operating the system, ensuring network information security and safety, and drafting, storing and transmitting State secrets via the information system; and responsibilities of each section and individual for management, operation and use; and remedies for strictly dealing with breaches.

Article 13 *Conditions on personnel operating and administering systems and protecting cybersecurity*

1 There must be a section in charge of operating and administering the system and protecting cybersecurity.

2 Personnel in charge of operating and administering the system and protecting cybersecurity must be assessed in terms of their ethics via their CVs or legal records; have professional qualifications in cybersecurity, network information safety and/or IT commensurate with their working positions; be provided with training on and dissemination of the regulations on cybersecurity; and commit to keep confidentiality of information relating to the critical information system during the period of employment and upon termination of employment.

3 Independent operational mechanisms must be formulated between the personnel section performing the duty of administration and [the personnel section] operating the information system; and [between the personnel section] inspecting cybersecurity and [the personnel section] developing, administering and operating the information system.

Article 14 *Conditions for ensuring cybersecurity of equipment, hardware and software being system components*

1 [Equipment, hardware and software] are subject to inspection of cybersecurity in order to detect any weaknesses, security holes or intrusion codes, ensuring compatibility with other components of the critical information system.

2 It is not permitted to use any product for which the CTF has provided a warning of the possibility of a loss of cybersecurity or for which it is required to take measures for dealing with or remedying any weaknesses, security holes or intrusion codes before putting such product into use.

3 Digital data or information which is processed or stored via an information system and is classified as State secret must be encoded or there must be measures for protecting such data or information during the process of creation, exchange and storage.

4 IT equipment, means of communications, media and equipment servicing operations of the information system must be closely managed in accordance with regulations of the information system administrator.

5 System software, utility software, middleware, databases, application programs, source codes and development tools are periodically reviewed and updated with security patches.

6 Mobile devices, upon connecting to the intranet system of the critical information system, must be inspected and controlled to ensure safety, and must be used in the critical information system only.

7 With respect to information storing equipment and/or means, it is required to:

(a) Check confidentiality before connecting information storing equipment and/or means to the critical information system;

(b) Control the connection of information storing equipment and/or means to or disconnection of same from equipment of the critical information system;

(c) Take measures for ensuring safety of information storing equipment and/or means when transporting and/or storing same;

(d) Take measures for protecting confidential information stored in information storing equipment and/or means.

Article 15 *Conditions on technical measures for cybersecurity supervision and protection*

1 The operating environment of a critical information system must satisfy the following requirements:

(a) Be separate from development, checking and testing environments;

(b) Apply solutions to ensure information safety;

(c) Not install application development tools or means;

(d) Remove or turn off functions and utility software which are not used in the information system.

2 With respect to data of a critical information system, there must be an appropriate automatic backup plan in external storage means [commensurate] with the changing frequency of such data, and it must ensure the principle that any data generated must be backed up within twenty four (24) hours. Backup data must be checked once every six (6) months, ensuring the ability to recovery such data.

3 A network system must satisfy the following requirements:

(a) Separate into different areas depending on the category of users and the use purpose, in which there must be at least a separate network zone for the server of the information system, a demilitarized zone (DMZ) for providing services on the Internet, and a separate network zone for providing wireless network services;

(b) Install devices and/or software to perform the function of controlling any connection or access to important network zones;

(c) Install devices and/or software to perform the function of connecting to, detecting and preventing intrusion from an untrusted network to the critical information system;

(d) Have solutions to control, detect and promptly prevent any unauthorized connection and/or access to the critical information system;

(dd) Have a load balancing plan and a plan for responding to denial-of-service [DoS] attacks and other forms of attack in conformity with the scale and/or nature of the critical information system.

4 It is required to formulate measures and/or solutions to search and promptly detect any technical weaknesses and/or vulnerabilities of the network system and any connection, equipment and/or software illegally installed in the network.

5 It is required to record and store the operational log of the information system and of users, of errors which arise and of information safety incidents for at least three (3) months in a centralized manner and carry out backup at least once every year.

6 It is required to control access with respect to persons or groups of persons using equipment and tools [for access] as follows:

(a) Register, grant, renew and revoke access rights of equipment and users;

(b) Each account accessing the system must be attributed to one single user; the sharing of a joint account to access the critical information system must be approved by the competent level and personal liability must be able to be determined at each time of use;

(c) Restrict and control accesses using accounts with administrator's rights: (i) A mechanism to control the creation of accounts with administrator's rights is established to ensure that no account can be used without approval by the competent level; (ii) There must be measures to supervise the use of accounts with administrator's rights; (iii) The use of accounts with administrator's rights must be restricted to ensure that there is only one single access with administrator's rights with automatic logout from the login session where there is no activity during a certain period of time;

(d) Manage and issue passwords to access the information system;

dd) Review, check and re-approve access rights of users;

(e) [Regulate] requirements and conditions on information safety with respect to equipment and tools used for access.

Article 16 *Conditions on physical security*

1 [The information system] must be situated and installed in a safe location and must be protected to minimize any risks resulting from environmental threats and/or dangers and illegal infiltration.

2 Power sources and supporting systems must be ensured when the main power source is interrupted; there must be measures for preventing overload, voltage sag or lightning spread; there must be a grounding system; there must be a backup generator system and an uninterruptible power supply system to ensure continuous operation of equipment.

3 There must be plans and measures to protect and prevent any trespass of unmanned aerial vehicles – UAV for collecting information.

4 There must be persons controlling and protecting the data center 24 hours per 7 days.

CHAPTER 3

Sequence and Procedures for Evaluating, Assessing, Inspecting, Responding to and Remedying Cybersecurity Incidents

Article 17 *Evaluation of cybersecurity*

1 The sequence for evaluation of cybersecurity of a critical information system is as follows:

(a) The administrator of the critical information system submits an application file requesting evaluation of cybersecurity to the competent Cybersecurity Task Force [CTF];

(b) The CTF receives, checks and provides guidelines for completing the file;

(c) The CTF conducts evaluation of cybersecurity in accordance with the contents stipulated in article 11.3 of the *Law on Cybersecurity* and notifies the results within sixty (60) working days from the date of issuance of the receipt for the file from the administrator of the critical information system.

2 The application file requesting evaluation of cybersecurity of a critical information system comprises:

(a) Written request for evaluation of cybersecurity;

(b) Pre-feasibility study report and design file for construction/building of the works of the investment project for construction of the information system prior to approval;

(c) Plan on upgrading the information system prior to approval in the case of upgrade of a critical information system.

3 Where necessary, the CTF shall conduct a survey and assess the actual status of the critical information system to check against the application file. Such survey and assessment must not affect normal operations of the administrator as well as of the critical information system.

4 With respect to information systems not included in the list of critical information systems, the evaluation of cybersecurity shall be decided by administrators of such information systems.

Article 18 *Assessment of cybersecurity conditions*

1 Administrators of information systems shall decide to assess cybersecurity conditions with respect to information systems under their management in accordance with Section 3 of Chapter II of this Decree, except for critical information systems.

2 The sequence for assessment of cybersecurity conditions with respect to a critical information system is as follows:

(a) The administrator of the critical information system submits an application file requesting assessment of cybersecurity conditions with respect to the critical information system to the CTF authorized to assess cybersecurity conditions as prescribed in article 12.3 of the *Law on Cybersecurity*;

(b) The CTF conducting assessment of cybersecurity conditions receives, checks and provides guidelines for completing the application file;

(c) Upon receipt of a complete and valid file, the CTF conducts assessment of cybersecurity conditions and notifies the results within fifteen (15) working days from the date of issuance of the receipt for the complete and valid file from the administrator of the critical information system;

(d) Where all cybersecurity conditions are satisfied, the head of the agency conducting assessment of cybersecurity conditions issues a certificate of satisfaction of cybersecurity conditions with respect to the critical information system within three (3) working days from the date of completion of assessment of cybersecurity conditions.

3 The application file requesting certification of satisfaction of cybersecurity conditions with respect to a critical information system comprises:

(a) Written request for certification of satisfaction of cybersecurity conditions;

(b) Design file and file on solutions for ensuring cybersecurity of the critical information system.

4 Where cybersecurity conditions are not satisfied, the CTF conducting assessment of cybersecurity conditions requests the administrator of the critical information system to supplement and/or upgrade the critical information system in order to satisfy all [cybersecurity] conditions.

Article 19 *Inspection of cybersecurity*

1 Administrators of information systems decide to inspect cybersecurity of information systems under their management, except for critical information systems.

(a) Cases in which cybersecurity is inspected and items subject to an inspection of cybersecurity shall be as prescribed in clauses 1 to 3 of article 13 and article 24.1 of the *Law on Cybersecurity*;

(b) The contents of inspection of cybersecurity comprise the following: inspection of compliance with the provisions of law on ensuring cybersecurity and protecting State secrets in cyberspace; inspection and assessment of the efficiency of plans and/or measures for ensuring cybersecurity, and options and/or plans for responding to and remedying cybersecurity incidents; inspection and assessment of detected security holes and weaknesses and intrusion codes, and system penetration testing attacks; and other inspections and assessments as stipulated by the administrator of the information system.

2 The sequence and procedures for an extraordinary inspection of cybersecurity by the CTF are as follows:

(a) Provide a notice of the plan on inspection of cybersecurity;

(b) Establish an inspection team in accordance with assigned functions and duties;

(c) Conduct inspection of cybersecurity, and coordinate closely with the administrator of the information system during the process of inspection;

(d) Prepare the minutes of the process and results of inspection of cybersecurity and keep same in accordance with law;

(dd) Notify the results of inspection of cybersecurity within seven (7) working days from the date of completion of inspection.

3 If it is required to maintain the current status of the information system for the purpose of investigating and/or dealing with any breach of law, the CTF shall send a letter requesting the administrator of the information system temporarily suspend the inspection of cybersecurity. Such letter must specify the reasons, purpose and duration of temporary suspension of inspection of cybersecurity.

Article 20 *Responding to and remedying cybersecurity incidents*

1 Administrators of information systems shall decide to respond to and/or remedy cybersecurity incidents with respect to information systems under their management, except for critical information systems.

2 When a cybersecurity incident of a critical information system is detected:

(a) The CTF shall send a written notice thereof to the administrator of the critical information system.

In a case of emergency, the notification may be made by telephone or other methods before sending a written notice.

(b) The administrator of the critical information system is responsible to remedy the cybersecurity incident immediately after receiving the notice, except for the provision in sub-clause (c) below.

If [such cybersecurity incident] is beyond the ability [of the administrator of the critical information system], it must be promptly notified to the CTF for coordinating, responding to and remedying the cybersecurity incident;

(c) Where necessary, the CTF shall decide to directly coordinate, respond to and remedy the cybersecurity incident.

3 The CTF shall coordinate, respond to and remedy a cybersecurity incident as follows:

(a) Assess and decide a plan for responding to and remedying the cybersecurity incident;

(b) Operate the work of responding to and remedying the cybersecurity incident;

(c) Preside over receiving, collecting, processing and exchanging information about responding to and remedying the cybersecurity incident;

(d) Mobilize relevant organizations and individuals to participate in responding to and remedying the cybersecurity incident where necessary;

(dd) Appoint an entity acting as the contact point to coordinate with functional entities of other nations or international organizations in responding to and remedying inter-nation incidents;

(e) Inspect, supervise and monitor the implementation of response to and remedying of the cybersecurity incident by the relevant entities.

4 Any organization or individual participating in responding to and remedying a cybersecurity incident is responsible to take measures for and carry out activities of responding to and remedying the incident as coordinated by the CTF.

5 Telecom enterprises and enterprises providing services on the Internet shall arrange sites, connection ports and technical measures required to the CTF under the MPS to perform the duty of ensuring cybersecurity.

CHAPTER 4

Implementation of Cybersecurity Protective Activities in State Agencies and Political Organizations at the Central and Local Levels

Article 21 *Formulation and completion of rules and regulations on use of computer networks of State agencies and political organizations at the central and local levels*

1 Administrators of information systems of State agencies and political organizations at the central and local levels must formulate rules and regulations on using, managing and ensuring security of intranets and internet-connected computer networks under their management. The contents of such rules and regulations shall be based on the regulations on protection of cybersecurity, protection of State secrets, technical standards and regulations on network information safety and other relevant specialized technical standards.

2 Rules and regulations on using and ensuring security of the computer network of a State agency or political organization at the central or local level must contain the following basic particulars:

(a) Clearly identify the information network system and important information for which the assurance of cybersecurity is required to be prioritized;

(b) Clearly stipulate prohibitions and principles for managing, using and ensuring cybersecurity, including the provision that the intranet which stores and transmits State secrets must be totally physically separated from internet-connected computer networks and electronic means and equipment;

(c) Managerial, professional and technical procedures for operating, using and ensuring cybersecurity of data and technical infrastructure, satisfying the basic requirements on ensuring safety of information systems;

(d) Conditions on personnel, especially personnel administering the network, operating the system, and ensuring cybersecurity and information safety, and involved in activities of drafting, storing and transmitting State secrets via the computer network system;

(dd) Clearly stipulate responsibilities of each section, officer and staff member in managing, using and ensuring cybersecurity and information safety;

(e) [Stipulate] remedies for dealing with breaches of the regulations on ensuring cybersecurity.

Article 22 *Formulation and completion of plans for ensuring cybersecurity of information systems of State agencies and political organizations at the central and local levels*

1 Heads of State agencies and political organizations at the central and local levels are responsible to promulgate plans for ensuring cybersecurity of information systems under their management, and to ensure completeness, consistency, centralization, common use and sharing of resources for the purpose of optimizing the efficiency and avoiding overlapping investment.

2 Subject to the importance of an information system and/or information stored and transmitted on the information system, a plan for ensuring cybersecurity of the information system may contain the following contents:

(a) Regulations on ensuring cybersecurity during design and construction of the information system, satisfying basic requirements such as managerial, technical and professional requirements;

(b) Evaluation of cybersecurity;

(c) Inspection and assessment of cybersecurity;

(d) Supervision of cybersecurity;

(e) Backup, response to and remedy of cybersecurity incidents and dangerous cybersecurity situations;

(g) Risk management;

(h) Termination of operation, exploitation, repair, liquidation and cancellation.

Article 23 *Plans for responding to and remedying cybersecurity incidents of State agencies and political organizations at the central and local levels*

1 Subject to the importance of an information system and/or information stored and transmitted in the information system, a plan for responding to and remedying cybersecurity incidents may include the following plans:

(a) Plan for preventing and dealing with information with contents posted in the information system which carry propaganda against the State of the Socialist Republic of Vietnam; which incite riots, disrupt security or cause public disorder; which are humiliating or slanderous; or which violate economic management order;

(b) Plan for preventing and combatting cyberespionage; and protecting information classified as State secret, work secrets, business secrets, personal secrets, family secrets and private life in the information system;

(c) Plan for preventing and combatting use of cyberspace, information technology and electronic media in order to breach the law on national security, social order and safety;

(d) Plan for preventing and combating cyberattacks;

(dd) Plan for preventing and combating cyberterrorism;

(e) Plan for preventing and dealing with dangerous cybersecurity situations.

2 Contents of a plan for responding to and remedying cybersecurity incidents [comprise]:

(a) General provisions;

(b) Assessment of cybersecurity threats and incidents;

(c) Plan for responding to and remedying a number of specific situations;

(d) Duties and responsibilities of [the concerned] agencies for organization of, coordination of, dealing with, responding to and remedying incidents;

(dd) Training, drills, prevention of incidents; and supervision, detection, and guarantee of conditions for readiness to respond to and remedy, incidents;

(e) Solutions for ensuring and organizing implementation of options and plans, and funding for implementation.

3 Activities of responding to and remedying cybersecurity incidents of information systems of State agencies and political organizations at the central and local levels shall be implemented in accordance with article 15.1 of the *Law on Cybersecurity*.

CHAPTER 5

Storing Data and Having Branches or Representative Offices in Vietnam

Article 24 *Data required to be stored in Vietnam*

1. Data on personal information of service users in Vietnam, including: full name, date of birth, place of birth, nationality, profession, position [title], place of residence, contact address, email address, telephone number, people's identity card number, personal identification number [PIN], citizen's identity card number, passport number, social insurance card number, credit card number, health status, medical history record, and biometrics.

2. Data generated by service users in Vietnam, including: information chosen to be uploaded, synchronized or imported from a device;

3. Data about the relationships of service users in Vietnam, including: friends, and groups with which the user connects or interacts.

Article 25 *Enterprises required to store data and have branches or representative offices in Vietnam*

1 Any domestic or foreign enterprise which satisfies all the following conditions must store data and have its head office, branches or representative offices in Vietnam:

(a) It is an enterprise which provides one of the services on telecom network, on the Internet, or added services in cyberspace with the following business activities in Vietnam: telecom services; services of data storage and sharing in cyberspace; supply of national or international domains to service users in Vietnam; e-commerce; online payment; intermediary payment; service of transport connection via cyberspace; social networking and social media; online electronic games; email;

(b) It carries out activities of collecting, exploiting [using], analysing and processing the types of data prescribed in article 24 of this Decree;

(c) It allows service users to conduct the acts prescribed in articles 8.1 and 8.2 of the *Law on Cybersecurity*;

(d) It breaches the provisions in article 8.4, or article 26.2(a) or article 26.2(b) of this Decree and has a branch or representative office in Vietnam.

2. The Minister of Public Security [MPS] requires that enterprises which satisfy the conditions in clause 1 above store the data prescribed in article 24 of this Decree and have a branch or representative office in Vietnam.

3. Enterprises which do not comply with the provision in clause 2 above shall, subject to the nature and seriousness of the breach, be dealt with in accordance with law.

Article 26 *Period for storing data*

1 The system log prescribed in article 26.2(b) of the *Law on Cybersecurity* must be stored for a minimum period of twelve (12) months.

2 The period for storing data prescribed in article 24.1 of this Decree shall be the operational duration of the enterprise or until services are no longer provided.

3 The period for storing data prescribed in clauses 2 and 3 of article 24 of this Decree is at least thirty six (36) months.

CHAPTER 6

Implementing Provisions

Article 27 *Ensured funding*

1 The funding for ensuring cybersecurity in the operation of central and local State agencies and political organizations is ensured by the State budget.

2 Funding invested in cybersecurity using public investment capital is implemented in accordance with the *Law on Public Investment*. With respect to public investment projects for new construction, or expansion or upgrading of information systems, investment funding is arranged in the investment capital of the corresponding project.

3 Funding for implementation of evaluation, supervision, checking and assessment of cybersecurity conditions; and for implementation of cybersecurity ensuring plans of central and local State agencies and political organizations is reconciled and arranged in the annual estimated budget of such agencies and organizations as delegated by the *Law on the State Budget*.

4 The Ministry of Finance provides guidelines for expense items for cybersecurity work in estimated budgets, and for management and use of professional budget for cybersecurity work of State agencies and organizations.

5 Based on their assigned duties, State agencies and organizations prepare their estimated budgets, manage, use and finalize the funding for implementation of the cybersecurity ensuring duty in accordance with the *Law on the State Budget*.

Article 28 *Effectiveness*

This Decree is of full force and effect as from 1 January 2019.

Article 29 *Transitional provision*

Within twelve (12) months from the date of request by the Minister of Public Security, the enterprises prescribed in article 25 of this Decree must store data and have a branch or representative office in Vietnam.

Article 30 *Responsibility for implementation*

1 The Minister of Public Security monitors, inspects and guides the implementation of this Decree.

2 Ministers, heads of ministerial equivalent agencies and of Government agencies, and chairmen of people's committees of provinces and cities under central authority are responsible to implement this Decree.

For the Government
Prime Minister
[NGUYEN XUAN PHUC]