Data Law 2024

Currently, in Vietnam, there are many Laws, including Law on Electronic Transactions, the Law on Cybersecurity, Law on Cyberinformation Security, Law on Telecommunications, and Law on Information Technology regulating databases, including national databases and specialized databases. However, all existing Laws do not specifically or consistently regulate data processing and management, such as data collection, digitization, quality assurance, data storage, etc.); do not regulate the development platform and application of high technology in data processing; do not regulate the creation of databases compiled from national databases and specialized databases; has not yet regulated the products and services related to data which are developing in the world such as data exchanges, data intermediary services, data analysis and synthesis services, etc. Meanwhile, the establishment of a data market, the construction and development of products and services related to data in Vietnam today plays a very important role, it is considered a breakthrough factor to gradually create and promote the opening of the data market in Vietnam, using the data market as a driving force for data development, promoting digital transformation (not only for the State agencies but also for enterprises) in all sectors and fields in Vietnam.

For above-mentioned purposes, along with collection of public opinions to finalise the draft Law on Personal Data Protection, on 30 November 2024, the National Assembly passed Data Law No.60/2024/QH15 (“Data Law”). The Data Law shall take effect on 1 July 2025 and applies not only to: (a) Vietnamese agencies, organizations and individuals; and (b) Foreign agencies, organizations and individuals in Vietnam; but also to (c) Foreign agencies, organizations and individuals directly participating in or related to digital data activities in Vietnam.

Within the scope of this article, we would like to summarize some notable contents of the Data Law as follows:

1. Interpretation

The Data Law provides several new definitions such as:

(a) “Digital data” is data about objects, phenomena, events, including one or a combination of sounds, images, numbers, writings, symbols expressed in digital form (hereinafter referred to as data).
(b) “Open data” is data that any agency, organization, or individual, if necessary, can access, share, exploit, and use.
(c) “Original data” is data created during the operation of an agency, organization, or individual or collected and created from digitizing original documents, papers, and other forms of material.
(d) “Important data” is data that can impact national defence, security, foreign affairs, macroeconomics, social stability, health, and public safety in the list issued by the Prime Minister;
(e) “Core data” is important data that directly affects national defence, security, foreign affairs, macroeconomics, social stability, health and public safety in the list issued by the Prime Minister of Government;
(f) “Data administrator” is an agency, organization or individual that carries out activities of building, managing, operating and exploiting data at the request of the data owner;
(g) “Data owner” is an agency, organization or individual that has the right to decide on the building, development, protection, administration, processing, use and exchange of the value of the data he/she/it owns;
(h) “Data owner’s rights to data” are property rights as prescribed by civil law.

in which there are some definitions different from the provisions of Decree No. 13/2023/ND-CP dated 14 July 2023 on

Personal Data Protection, such as:

(a) “Data subject” is an agency, organization, or individual reflected by data; and
(b) “Data processing” is the process of receiving, converting, organizing data, and other activities related to data to serve the operations of agencies, organizations, or individuals.

2. Principles of Application

The Data Law stipulates that in the cases where another Law promulgated before the effective date of the Data Law has provisions that are not contrary to the principles of this Law, the provisions of that Law shall be implemented. If such Law has provisions different from those of the Data Law, it is necessary to specifically identify the content of implementation or non-implementation according to the provisions of the Data Law and the content of implementation according to the provisions of that other Law. Thus, the Data Law does not provide for handling the cases where other laws enacted before the effective date of the Data Law contain the provisions contrary to the principles of the Data Law.

3. Data Processing

3.1. Data Collection and Creation

The Data Law stipulates that:

(a) Data is collected and created from sources, including: direct creation; and digitization of documents, papers and other forms of material. The original data created has the same value as the original documents, papers and other forms of material that are digitized.
(b) Organizations and individuals have the following rights and responsibilities regarding data collection and creation activities: (i) Collecting and creating data to serve their activities in accordance with the provisions of law; (ii) Having the rights of data owners protected according to the

provisions of the Data Law, provisions of civil laws and other relevant provisions of law; and (iii) Being responsible for the data they collect and create according to the provisions of law.

3.2. Data Classification

Data owners and data administrators who are not the State agencies must classify data according to the importance of the data into: core data, important data, and other data; and classify data according to other criteria. The Government will prescribe criteria for determining core data and important data.

3.3. Provision of Data to the State Agencies

Organizations and individuals must provide data to the State agencies when requested by competent authorities without the consent of the data subject in one of the following cases: (a) Responding to a state of emergency; (b) When there is a threat to national security but not to the extent of declaring a state of emergency; (c) Disaster; (d) Preventing and combating riots and terrorism. The State agencies receiving data are responsible for: (a) Using the data for proper purpose; (b) Ensuring data security, safety, data protection, and other legitimate interests of data subjects, organizations, and individuals providing data in accordance with the provisions of law; (c) Destroying data immediately when the data is no longer necessary for the requested purpose and notifying the data subjects and organizations or individuals providing the data thereof; and (d) Notifying the storage and use of data upon request of organizations and individuals providing the data, except in cases of protecting the State secrets and work secrets.

3.4. Data Certification and Authentication

Data certification is performed by the data owner, data administrator or electronic authentication service provider.

Certified data has the value of proving the existence, time and storage location of data in cyberspace according to the provisions of the Data Law and other relevant provisions of law.

Data authentication is performed by the data owner, data administrator who creates the original data, electronic authentication service provider, or the National Data Centre. Authenticated data has the same value as the original data stored in the national database, specialized database or other database within a certain scope and time.

3.5. Data Encryption and Decryption

Data in the list of State secrets must be encrypted using cryptographic codes when stored, transmitted, received, and shared on computer networks. The data owner or data administrator decides to encrypt and decrypt data using one or more encryption solutions and encryption and decryption processes appropriate to their data administration and management activities. However, the competent State agencies are entitled to apply measures to decrypt data without the consent of the data owner or of data administrator in one of the following cases: (a) State of emergency; (b) When there is a threat to national security but not to the extent of declaring a state of emergency; (c) Disaster; and (d) Prevention and control of riots and terrorism; as prescribed by the Government.

3.6. Cross-border Transfer of Data

Agencies, organizations and individuals may freely transfer data from abroad to Vietnam, process foreign data in Vietnam, and have their legitimate rights and interests protected by the State in accordance with the provisions of law. The cross-border transfer and processing of core data and important data, including: (a) Transferring data stored in Vietnam to data storage systems located outside the territory of Vietnam;

(b) Vietnamese agencies, organizations and individuals transferring data to foreign organizations and individuals; and (c) Vietnamese agencies, organizations and individuals using platforms outside the territory of Vietnam to process data must ensure national defence, security, protect national interests, public interests, rights and legitimate interests of data subjects and data owners in accordance with the provisions of Vietnamese laws and international treaties to which Vietnam is a member.

3.7. Identification and Management of Risks Arising in Data Processing

Risks arising in data processing include: privacy risks, network security risks, identification and access management risks, and other risks implied in data processing. Data owners who are not the State agencies shall self-assess, identify risks, and implement measures to protect data; promptly remedy risks that arise and notify to data subjects, relevant agencies, organizations, and individuals. Owners of core data and important data must periodically conduct risk assessments for such data processing activities according to the regulations and notify to specialized units on cybersecurity and information security under the Ministry of Public Security, Ministry of National Defence, and relevant agencies to coordinate in implementing data safety and security protection.

3.8. Other Activities in Data Processing

Data owners and data administrators who are not the State agencies are responsible for establishing procedures and implementing measures and methods to retrieve, delete or destroy data at the request of data subjects.

4. Data protection

Data protection measures are applied throughout the entire data processing process, including:

(a) Developing and organizing the implementation of data protection policies and regulations;
(b) Managing data processing activities;
(c) Developing and implementing technical solutions;
(d) Training, fostering, developing, and managing human resources; and
(e) Other data protection measures as prescribed by law.

Data owners as well as data administrators managing core data and important data must comply with the data protection regulations.

5. Data Exploitation

Data in the National General Database has the same value of exploitation and use as original data. Organizations and individuals who are not: (i) Vietnam Communist Party agencies, the State agencies, or socio-political organizations; and (ii) Data subjects; may freely to exploit and use open data; exploit and use personal data with the consent of the National Data Centre and individuals who are the subjects of exploited data; exploit and use other data with the consent of the National Data Centre. Data exploitation and use are carried out through the following methods: (i) Connecting and sharing data between national databases, specialized databases, databases, information systems other than the National General Database; (ii) National Data Portal, National Public Service Portal, electronic information portal, information system for processing administrative procedures; (iii) Electronic identification and authentication platform; (iv) National identification application; (v) Equipment, means, software provided by the National Data Centre; and (vi) Other methods.

Organizations and individuals exploiting and using their own data in the National General Database and other databases managed by the State agencies are not required to pay fees. Organizations and individuals that are not Vietnam Communist Party agencies, the State agencies or socio-political

organizations exploiting and using data of other organizations and individuals in the National General Database and other databases managed by the State agencies must pay fees in accordance with the provisions of laws on fees and charges.

6. Data Products and Services

(a) The Data Law for the first time defines data products and services; including:

(i) Data intermediary

Data intermediary products and services are products and services that establish commercial relationships between data subjects, data owners and users of products and services, through agreements for the purpose of exchanging, sharing, accessing data, and exercising the rights of data subjects, data owners and data users. Organizations providing data intermediary products and services must be registered for operation and managed in accordance with the provisions of the law on investment; except for cases of providing data intermediary products and services within the organization.

(ii) Data analysis and synthesis

Data analysis and synthesis products are the result of the process of analysing and synthesizing data into useful in-depth information at different levels according to the requirements of the product users. Data analysis and synthesis services are the activities of analysing and synthesizing data according to the requirements of the service users. Organizations that trade in data analysis and synthesis products and services that may cause harm to national defence, security, social order and safety, social ethics, and public health must register their operations and be managed according to the provisions of the laws on investment.

(iii) Electronic authentication

Electronic authentication services perform data authentication in national databases, specialized databases, electronic identification and authentication systems provided by public non-business professional service units and the State-owned enterprises that meet the conditions for provision of this service.

(iv) Data trading floor

The organization providing data trading floor services is a public non-business professional service unit or State-owned enterprise that meets the conditions for provision of this service and is licensed to establish in accordance with the provisions of law. Data that is not allowed to be traded includes: (i) Data that is harmful to national defence, security, foreign affairs, and cryptography; (ii) Data which are not agreed to by data subjects, unless otherwise provided by law; and (iii) Other data that is prohibited from being traded in accordance with the provisions of law; and will be detailed by the Government.

(b) In addition, the Data Law also stipulates the rights and obligations of organizations providing data products and services. Accordingly,

(i) Organizations providing data intermediary products and services, data analysis and synthesis enjoy the same incentives as enterprises operating in the fields of high technology, innovation, creative start-ups, and digital technology industry.
(ii) Organizations providing data intermediary products and services, data analysis and synthesis service, and data trading floor service also have a number of responsibilities such as: Providing services to organizations and individuals on the basis of agreements in service provision contracts; Ensuring information reception channels and smooth and continuous use of services; Monitoring behaviours that may affect data protection; etc./.