KPMG

Legal Alert

April 2023

Decree 13/2023/ND-CP on Personal Data Protection is now released

On 17 April 2023, the Government issued the long-awaited Decree 13/2023/ND-CP on Personal Data Protection ("**Decree 13**"), which will take effect from **01 July 2023**. With the Law on Cybersecurity (before 4/2018/QH14) dated 12 June 2018 and its first implementing Decree 53/2022/ND-CP dated 15 August 2022, Decree 13 forms the third legal document issued in the Government's initiative to strengthen the legal framework governing cyberspace. Decree 13 provides more detailed data protection and cybersecurity obligations with respect to personal data processing activities.

Who needs to comply?

Decree 13 applies to any domestic or foreign organizations or individuals that are involved in processing personal data in Vietnam (e.g., employees, customers, suppliers, users, or other individuals), even if the processing occurs outside of Vietnam.

Whilst Decree 13 has similar requirements compared to the European Union's General Data Protection Regulation ("**GDPR**"), there are some significant differences, such as requirements for cross border transfers, consent forms and impact assessment reports, and lawful basis for processing personal data.

Companies that have privacy management practice and policies in place that are either GDPR-compliant or compliant with other privacy laws are not automatically granted a free pass as to compliance with Decree 13. With the effective date of 1 July 2023, businesses should begin reviewing their internal privacy management practices and policies immediately to identify gaps and a corresponding action plan.

How to comply?

We have outlined in the below table some of the key compliance requirements of Decree 13. Note that many of the provisions in this Decree are broadly worded and interpreting the same will be challenging. Given the short time for implementation, we expect that the Ministry of Public Security ("**MPS**") will issue further guidance on how Decree 13 is interpreted and enforced. These guidelines will assist businesses compliance efforts. We will continue to closely monitor the developments and provide updates. In the interim, there are various steps that businesses can take immediately to comply with Decree 13.

Action item	Compliance action required	Description
Identify role in processing personal data	Assign responsibility and protocols for every processing activity to the relevant business units. Review the data processing and recording techniques e.g., whether it is transactional, real time, batch, or multi-processing	Aligning with the definitions found in the GDPR, Decree 13 clearly distinguishes between the different roles of data handlers and have accorded separate responsibilities for each role. Specifically: **Data Controller** refers to an organization or individual that decides the purpose and means of processing personal data. Data Controller has the higher responsibility to notify and cooperate with the authorities in case of personal data breaches. The Data Controller is ultimately accountable to the data subject and bears the burden of proving prior consent is obtained for all processing activities. **Data Processor** refers to an organization or individual that is engaged under a contract by the Data Controller to process personal data in accordance with the instructions of the Data Controller. Data Processor is responsible for notifying the Data Controller of any breaches and cooperating with the authority in case of breaches and investigations. **Data Controller cum Processor** is a hybrid role and will need to comply with the obligations of both Data Controller and Data Processor. **Third parties**, on the other hand, refers to individuals or entities other than the Data Controller or Data Processor that are allowed to process personal data. This definition may broadly refer to anyone that is permitted to be involved in personal data handling such as payment service providers, telecommunication service providers, etc.
Identify types of personal data processed	Develop or review internal data management structures and operating rules and set up a data categorization and management system for different types of personal data.	**Personal data** refers to information associated with a particular person or helps identify a natural person when used independently or combined with other information that can be the direct information, numbers, text, images, audio, video, and digital data. Decree 13 classifies personal data into two (2) types: (i) basic and (ii) sensitive personal data, and provides a non-exhaustive list of each classification. **Basic personal data** includes: usual identification information e.g., name, date of birth, date of death, contact details, marital status and family relationship, ethnicity, personal image, gender, personal identification numbers (citizen identification number, passport, tax code, social/medical insurance code, driving license number, vehicle plate number) but also including blood type, digital accounts and data reflecting individuals' activity history on cyberspace. **Sensitive personal data** is defined as personal data associated with an individual's privacy and when violated will directly affect the individual's legitimate rights and interests and includes political and religious views, health conditions (except blood type), biometric data, genetic data, sexual orientation, criminal records, customer data of credit institutions, intermediate payment services, geographic location and other types of sensitive personal data as stipulated by Vietnamese laws. Decree 13 imposes additional processing and safeguarding obligations for processing sensitive personal data
Identify lawful basis for personal data processing	The burden of proving that data is processed lawfully is on the entity processing the data. Consider if the existing practice, policies, training and system logs can demonstrate compliance. Internal rules and policies should include: rules and procedures for processing personal data; authorization for personnel to process data, rules and processes in case of personal data breaches, and remediation protocols.	As with the GDPR, Decree 13 generally requires organizations to obtain the individual's prior consent to process personal data and adhere to the principles set out in Article 3, namely process data (i) lawfully; (ii) transparently; (iii) for purpose(s) disclosed; (iv) limited purpose and scope; (v) using appropriate and updated data; and (vi) confidentially; whilst (vii) ensuring data is stored for the appropriate retention period, and (viii) be accountable. Of note, Decree 13 expressly prohibits purchase of any data that is likely intended to address the sale of data lists in the past. Essentially, save for a few exceptions, the data subject's consent is required to lawfully process personal data for all activities, including for cross marketing and advertising. A new consent is required each time the organization changes the way they are handling data.

Action item	Compliance action required	Description
	A mechanism is put in place to ensure consent is capable of being printed or reproduced in writing, which can be in electronic format. Assess if the form of consent complies with the requirements of Decree 13. If relying on other conditions to process, assess if the data subject will be notified.	Consent is valid if given through a positive and voluntary action (like signing, ticking a box, clicking a button) after the individual is given full information of how, and the extent of, the processing of personal data. Default setting, pre-ticked boxes, general terms and conditions or silence or non-response will not be considered as consent. The individual has the right to withdraw his or her consent at any time. Processing without consent is limited to the following circumstances: a. to protect the life and health of the data subject or others; b. disclosure in accordance with the law; c. by State agencies, such as (i) in the event of a state of emergency or when there is a risk of threatening national security and national defense; to prevent against riots and terrorism, to prevent against crimes and violations of the law; or (ii) to serve their activities, as prescribed by the law d. security surveillance with prior notification to the data subject to serve the data handler's legitimate purpose; e. to fulfil the contractual obligations (except to further its marketing and advertising business) of the data subject in accordance with the law. Apart from the general consent requirement, there are specific consent requirements from related parties in the following circumstances: a. children over the age of 7 will require the child and the guardian consent; and b. missing person or deceased will require consent from next of kin.
Implement mechanism for individuals to withdraw consent	Evaluate and update current mechanisms to guarantee this right; train employees responsible for handling data subject requests and raise personal data protection awareness. Where consent is used as a legal basis for processing personal data, to have a mechanism for individuals to withdraw their consent, which should allow for printing or re-production as needed. The system must have the ability to notify the individual of the consequence or damage that has arisen from the withdrawal.	Where consent is withdrawn, the organization will need to notify the individual of the possible consequence or damage that occurred as a result of the consent withdrawal.
Personal data processing notification requirements	Either review and update existing or develop new privacy policies containing minimum requirements prescribed by Decree 13 to provide to the individuals as soon as possible. Consult your legal advisors to ensure compliance.	Decree 13 requires organizations to provide a compliant notice to the individuals prior to processing their personal data. The privacy notice will need to include inter alia the type, purpose, and method of processing; identity of the data processor or third party involved; the risks of processing, the timing of the processing.
Implement system to handle data subject requests	A system through which the data subjects can exercise their rights and the appropriate personnel can receive, evaluate, authenticate, and respond to these requests.	Decree 13 provides data subjects with certain rights (e.g., to access, restrict, object, correct, delete, etc.) and requires data handlers to guarantee the data subjects these rights. Any request to restrict or objection to data processing will need to be addressed within 72 hours of the request.

Action item	Compliance action required	Description
Data protection officer	Appoint a data protection officer ("**DPO**") or designate a department with this compliance task.	Grace period for 2 years is only applicable for the case upon the establishment of micro-enterprises, small enterprises, medium-sized enterprises, startup companies which are not directly engaged in providing personal data processing services. Save for this, organizations are required to appoint a data protection officer.
Data security and data breach notification/ reporting	Depending on the role of the data handler, a system to detect, handle and notify the relevant authorities and affected data subjects in case of breach using the prescribed formats provided in Decree 13. Review contracts with Data Processors to check if it contains duties and obligations in relation to data protection and security and clarify how liability will be allocated between the parties.	Decree 13 requires **Data Controller and Data Controller cum Processor** to ensure that personal data security and notify the authorities of any personal data breaches within 72 hours of the breach occurring. On the other hand, Data Processors are required to notify Data Controllers immediately of a breach occurring to enable them to fulfil the 72- hour requirement. In case of delay, the Data Controller is required to provide reasons.
Impact assessment reports to authorities for personal data processing and cross border transfer	Review existing, or develop, personal information protection impact and risk assessment template in the format prescribed by Decree 13. The reports will need to be stored and be made available for inspection. Have a mechanism to ensure that these reports are produced and submitted within 60 days of commencement of processing activities or changes to the same.	Both Data Controllers and Data Processors must conduct a personal information impact assessment for all their processing activities, including processing basic and sensitive personal data on its own or by contracting a data processor or providing information to third parties or transferring personal data overseas and submit within 60 days of commencing the relevant processing activity. The impact assessment dossier must include: information on both the Data Controller and Data Processor and their internal DPO within the organization, recipients of the personal data and nationality, the types and purpose of personal data processed, the retention period, data protection measures, and risk assessment and mitigating measures for the processing activities. Data handlers will need to ensure that the impact assessment reports are available for review by MPS and be updated and supplemented in case any of the information it contains changes or evolves. If a violation is detected or if the transfer violates national interest or security, the MPS retains the discretion to stop any transfer overseas.
Investigations and audits	Have a mechanism and personnel tasked to handle any investigation and audit requests from the authorities.	Decree 13 provides the authorities broad power to conduct investigations and audit any data handlers' personal data management practices and policies on an annual basis or more if there is a need.

Contact us

Hanoi

46th Floor, Keangnam Landmark 72,
E6 Pham Hung, Me Tri, Nam Tu Liem

T +84 (24) 3946 1600

Ho Chi Minh City

10th Floor, Sun Wah Tower,
115 Nguyen Hue, Ben Nghe, District 1

T +84 (28) 3821 9266

Da Nang

Unit D3, 5th Floor, Indochina Riverside Towers,
74 Bach Dang, Hai Chau I, Hai Chau

T +84 (236) 351 9051

Scan to visit our website: kpmg.com.vn

Email: kpmghcmc@kpmg.com.vn