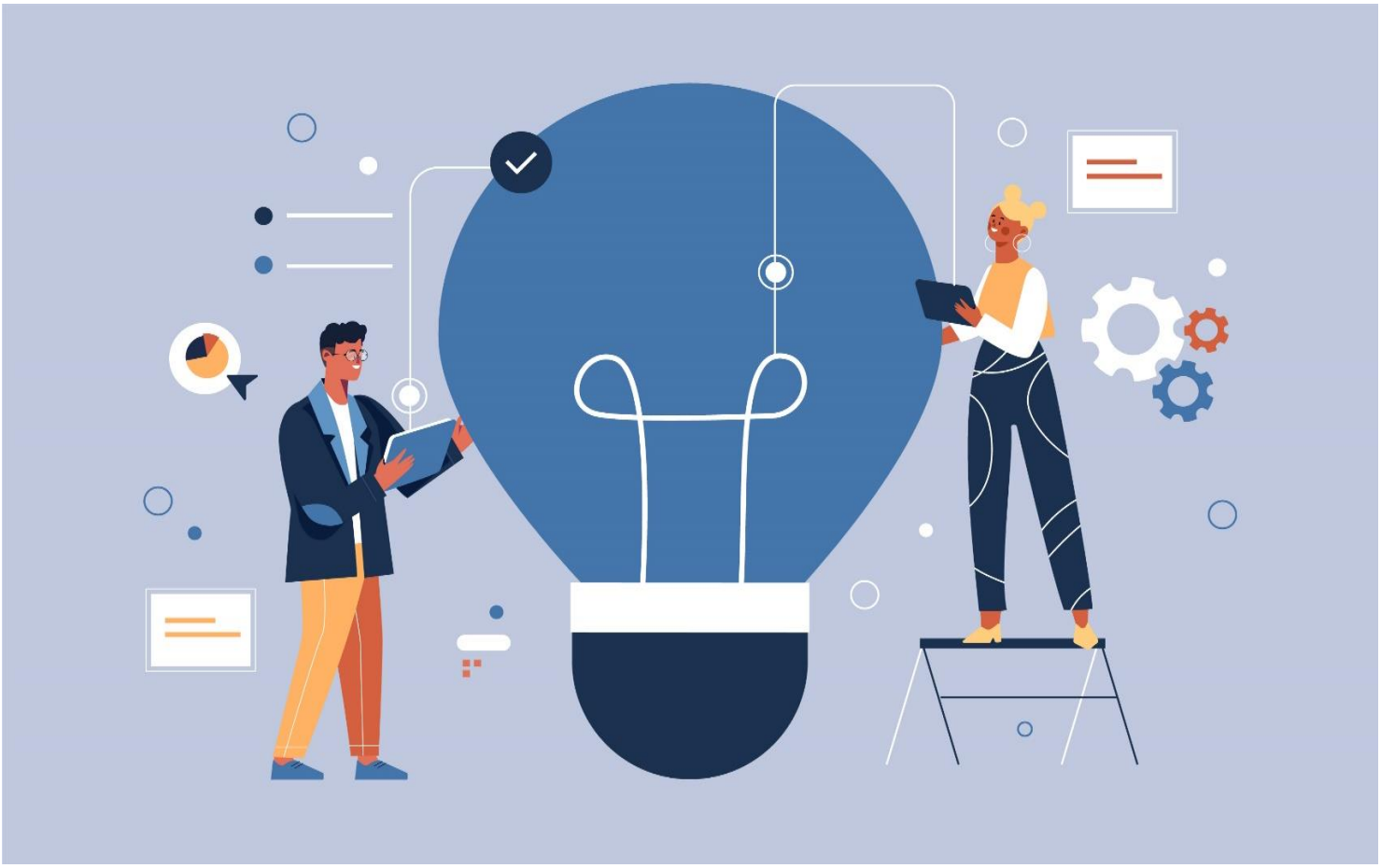
INSIDE THIS ISSUE

VIETNAM ENACTS DECREE 13: NEW PERSONAL DATA PROTECTION REQUIREMENTS FOR ORGANIZATIONS

OVERVIEW

The recent Decree No. 13/2023/ND-CP ("Decree 13") is a crucial legal tool for protecting personal data in Vietnam. Issued on 17 April 2023, Decree 13 brings in new requirements for safeguarding personal data. These requirements apply to all organizations, both domestic and foreign, as well as individuals involved in processing personal data in Vietnam. Decree 13 will come into force on 01 July 2023, with a two-year grace period for small and medium-sized enterprises regarding the obligation to appoint a data protection officer and department. Businesses need to review their internal privacy policies and compliance practices to ensure alignment with Decree 13 and to take prompt action to achieve compliance. Essential compliance requirements are detailed below.



DEFINING THE ROLE

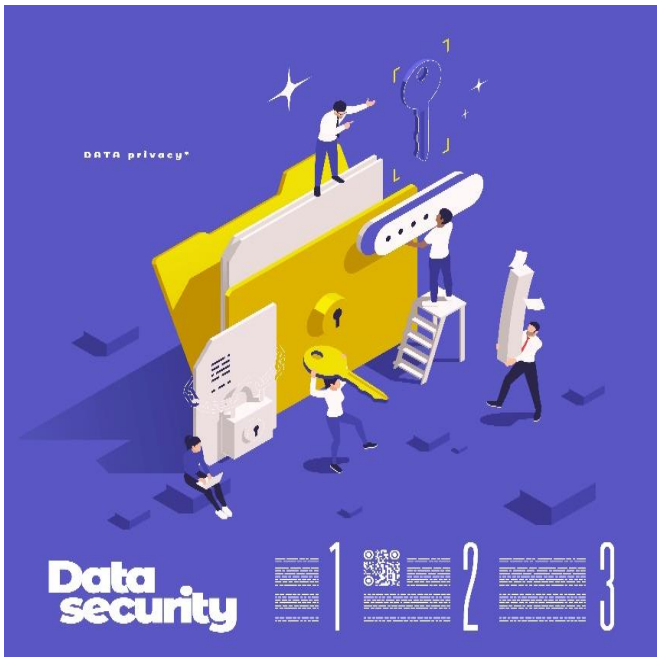
Under Decree 13, different parties involved in data processing have distinct responsibilities. The Data Controller, typically an organization or individual, determines the purpose and methods of processing personal information. They bear the highest responsibility for data protection compliance, including obtaining consent from data subjects for processing, addressing data subject requests, and reporting data breaches to the Ministry of Public Security (MPS).

On the other hand, a Data Processor processes personal data on behalf of the Data Controller through a contract. Their responsibilities include notifying the Data Controller of any breaches and processing data according to the contract terms.

A third role, the Data Controlling and Processing Party, combines aspects of the Data Controller and Data Processor roles.

Finally, Third Parties, which can be individuals or entities other than the data subject, Data Controller, Data Processor, or Data Controlling and Processing Party, may also process personal data. Their responsibilities include storing data in compliance with their operations and taking necessary measures to protect personal data as required by law.

Therefore, it is essential for businesses to clearly understand their specific roles in processing personal data to ascertain their responsibilities in this process.



ENSURING EXPLICIT CONSENT FOR DATA PROCESSING ACTIVITIES

Under Decree 13, obtaining the individual's explicit consent for all data processing activities is necessary, with only a few exceptions. The consent is considered valid only if freely given and if the data subject is fully informed about the type of personal data, the purpose of data processing, the parties involved in processing the data, and the rights and obligations of the data subject. It's important to note that consent can be given in various ways, such as in writing, verbally, by ticking a consent box, through text messages, by selecting technical settings, or by any other action that indicates the same. Silence or lack of a response from the data subject does not constitute consent. In a dispute, the burden of proving the data subject's consent lies with the Data Controller and the Data Controlling and Processing Party.

MANDATORY IMPACT ASSESSMENT DOSSIER

All organizations that handle personal data must create and maintain an Impact Assessment Dossier from the start of processing personal data. This dossier must be submitted to A05 for review within 60 days of processing and should be available for inspection by the MPS at all times. The dossier should contain information about the organization, data protection officer, purposes and types of personal data processed, recipients of personal data (including overseas entities), cases of cross-border data transfer, retention period, data protection measures, assessment of the impact of data processing, and potential consequences. Data Processors may also need to create and maintain this dossier based on contractual requirements with the Data Controller.

CONDITIONS FOR CROSS-BORDER TRANSFER OF VIETNAMESE CITIZENS' PERSONAL DATA

Decree 13 permits the transfer of personal data of Vietnamese citizens to a third country by the transferor (including the Data Controller, Data Controlling and Processing Party, Data Processor, and the Third Party), provided that certain conditions are met:

1. The transferor must create a dossier for impact assessment of cross-border personal data transfer processing. This dossier should contain essential details, such as a description of the types of personal data being transferred overseas, explanations of the objectives of processing the personal data of Vietnamese citizens, and a document outlining the binding responsibilities between the transferor and the recipient of the transferred personal data of Vietnamese citizens.

2. The impact assessment dossier must be accessible for review and inspection by the Ministry of Public Security (MPS) at any time. The transferor must submit the original impact assessment dossier in a specified format to the MPS within 60 days from the personal data processing date. If it is incomplete, MPS may request the transferor to complete the impact assessment dossier.

3. Following the successful transfer of data, the transferor must provide a written notification to MPS regarding the data transfer, along with the contact details of the person in charge.

4. MPS has the authority to suspend any cross-border transfer if the transferor fails to meet the requirements above, violates the interests and national security of Vietnam, or if there is any leakage or loss of Vietnamese citizens' personal data.

MANDATORY BREACH NOTIFICATION AND PENALTIES FOR DATA PROCESSORS

When inspecting any personal data breaches, the Data Processor must notify the Data Controller and the Department of Cybersecurity and Hi-tech Crime Prevention (MPS) within 72 hours of the breach. Notification should include specific details and be submitted in a prescribed format. If the notification is delayed, reasons for the delay must be provided. Specific administrative fines range from VND 10 million to VND 70 million for violations of regulations on personal data protection, with potential prosecution under the Penal Code for severe breaches.

CONCLUSION

The regulations outlined in Decree 13 impose substantial obligations on entities engaged in processing personal data, particularly multinational corporations. Due to the broad nature of these requirements, it is anticipated that the Ministry of Public Security (MPS) will provide additional guidance on how the provisions in Decree 13 should be interpreted and enforced.

DAITIN & ASSOCIATES

Lawyers and Consultants

CONTACT

Please contact Daitin & Associates if you require any further information or guidance in the procedures of acquiring, protecting intellectual property rights in Vietnam | Cambodia | Laos | Myanmar | Thailand | Philippines | Brunei | Indonesia.

info@daitin.com.vn | www.daitin.com.vn