ASIA COUNSEL INSIGHTS

May 2023

Asia Counsel Insights provide an overview of the key trending legal and business issues in Vietnam and how they may impact your business. Please enjoy your read.

Deal Update:

- Advising Kaizenvest on their investment in MindX, online tech education provider in the Series B fundraising round.

Personal Data Protection Decree

The Vietnamese Government has finally passed Decree No. 13/2023/ND-CP on personal data protection ("**Decree 13**") on 17 April 2023 after a two years' consultation process. Decree 13 will come into effect on 1 July 2023.

We will summarise the key issues of Decree 13 and the things that companies need to put in place in order to comply with Decree 13.

1. Scope of application

Decree 13 applies to both individuals, Vietnamese entities and organizations operating outside the territory of Vietnam directly participating in or related to personal data processing activities in Vietnam.

2. Classification of regulated subjects

Decree 13 classifies the following groups.

- Data Subject: is any individual who is identified by personal data;
- Data Controller: is any entity or individual who decides the purpose and means of processing data;
- Data Processor: is any entity or individual who processes data for the Data Controller under a contractual basis; and
- Data Controlling and Processing Entity: is any entity or individual who is a Data Controller and a Data Processor at the same time;
- Third parties: are other entities or individuals who process personal data.

Decree 13 sets out the rights and obligations of the above groups and it is important to identify which group that an entity belongs.

3. Categories of personal data

Personal data is classified into two categories: basic personal data and sensitive personal data.

Basic personal data includes, among others, name, date of birth, gender, place of birth, nationality, personal images, phone, identification number, marriage status, history of activities in cyberspaces of a person.

Sensitives personal data refers to privacy of an individual that, when infringed, directly affects the legitimate rights and interests of individuals. Sensitive personal data includes, among others, political and religious views, health status and private life recorded in medical records, ethnic origin, inherited genetic characteristics, sexual orientation, criminal records, customer information of credit institutions or branches of foreign banks or intermediary payment service providers, or data on location.

Data protection measures vary according to personal data classification.

4. Cross-border transfer of personal data

No prior regulatory approval is required for cross-border transfer of personal data.

However, Decree 13 requires the relevant entity that carries on cross-

About Asia Counsel

Asia Counsel is a dynamic international corporate and commercial law firm dedicated to serving clients in Vietnam. Our partners have over 14 years of experience in working on complex and challenging matters in Vietnam. We are committed to helping clients achieve their business strategies and providing outstanding legal services.
If you have any questions on any of the items discussed above, please do not hesitate to contact us.

Minh Duong
Managing Partner
E minh@asia-counsel.com

Ross Macleod
Partner
E ross@asia-counsel.com

Asia Counsel Vietnam Law Company Limited, Unit 9.10, Level 9, Deutsches Haus, 33 Le Duan Boulevard, Ben Nghe Ward, District 1, Ho Chi Minh City
www.asia-counsel.com

border transfer of personal data to prepare and archive an internal dossier to assess the impact of personal data transfer and have a copy submitted to the Department of Cyber Security and High-Tech Crime Prevention ("**A05**") of the Ministry of Public Security (MPS) within 60 days from the date of processing data. The relevant entity must also notify the A05 after the data is successfully transferred aboard.

5. Preparation for the effectiveness of Decree 13

The Data Controller, the Data Processor, the Data Controlling and Processing Entity ("**Applicable Entities**") must ensure that a range of measures are put in place to comply with Decree 13.

(a) Consents from Data Subjects

The Applicable Entities are required to develop a mechanism to obtain the consent from Data Subjects. The consents must be in a format that can be printed or copied in writing.

The Data Subjects' silence or non-response will not be regarded as consent, and the consent of the Data Subject is only valid when the Data Subject voluntarily and clearly knows the following:

- Type of personal data to be processed;
- The purposes for processing personal data;
- The relevant entities involved in the data processing; and
- Rights and obligations of data subjects.

However, the above consent requirements will not apply where the data processing is made in an emergency situation to protect the life and health of the Data Subject, a data disclosure in accordance with law, in order to fulfil contractual obligations of the Data Subjects; or in order to serve the activities of regulatory agencies.

The consent requirement is also exempted in case of data processing for purpose of national defence, security, social order and safety, disasters or dangerous epidemics.

(b) Data processing notification

The Applicable Entities are required to develop a mechanism for a one-time notification of the Data Subjects before processing data.

The contents of the notification include:

- processing purpose;
- type of data processed;
- processing method;
- information of relevant persons in relation to the processing purpose;
- the risk and likely impact of data breaches; and
- start time and end time of the data processing.

(c) Data protection measures

The Applicable Entities must implement measures to protect personal data and ensure the legitimate rights of the Data Subjects in accordance with Decree 13.

At the request of the Data Subject, the Applicable Entities must provide personal data of the Data Subject or require that certain data of the Data Subject be edited or deleted.

(d) Data protection department

The Applicable Entities are required to set up a personal data protection department and appoint a data compliance officer if they deal with sensitive personal data.

They also need to inform the A05 of such personal data protection department and compliance officer.

SMEs and start-up companies are exempted from setting up a personal data protection department and a data compliance officer for sensitive personal data within 2 years of establishment unless those companies directly operate in the data processing business.

(e) Cross-border transfer

The Applicable Entities are required to prepare a dossier and submit it to the A05 in case of cross-border transfer of personal data.

The contents of the dossier are below:

- Description and explanation of objectives of the processing of a Vietnamese citizen's data after the personal data is transferred;
- Description and clarification of the type of personal data to be transferred;
- Description and explanation of the observance of regulations on the protection of personal data, detailed measures for protecting personal data; and
- Documents showing obligations and responsibilities between the sender and the receiver in dealing with basic personal data or sensitive personal data and details of the personal data protection department and a data compliance officer if the applicant deals with sensitive personal data.

(f) Impact assessment on personal data processing

The Applicable Entities are required to prepare and archive an impact assessment on personal data processing ("**Assessment Dossier**"), and then submit the same to the A05 within 60 days upon commencing the data processing.

The Assessment Dossier include the documents below:

- Details of data protection department, compliance officer;
- Timeline of data processing;
- Whether there will be any cross-border transfer of personal data and in what circumstances;
- Data protection measures applied; and
- The risk of any data breaches and the mitigating measures if there is a data breach.