

## Draft New Decree on Personal Data Protection in Vietnam

On 9 February 2021, the Ministry of Public Security issued a draft decree on the protection of personal data ([Draft Decree](#)). This decree, once enacted, will be the first comprehensive legislation of Vietnam on personal data. This blog will analyze some key points of the Draft Decree and compare them with the relevant provisions under the General Data Protection Regulation (**GDPR**).<sup>1</sup> This post is written by Nguyen Thu Giang and edited by Nguyen Quang Vu.

### 1. Scope of application

1.1. While the GDPR lists out cases that are not governed by the GDPR, the Draft Decree tends to act as a catch-all for types of activities relating to personal data in Vietnam, both materially and territorially.

#### *Material scope*

1.2. Unlike the GDPR, the Draft Decree is silent on which cases can be exempted from personal data protection requirements. For example, the GDPR exempts, among others, the following cases from its governing scope:<sup>2</sup>

1.2.1. the processing of personal data by a natural person in the course of a purely personal or household activity; and

1.2.2. the processing of personal data by competent authorities for public purposes such as for the prevention, investigation, detection or prosecution of criminal offences.

1.3. Given this ambiguity, an individual maintains a contact list, which comprises of name, mobile number, email, in her phone purely for personal purposes, might still be subject to the Draft Decree.

#### *Territorial scope*

1.4. The Draft Decree is also silent on its territorial scope. On the contrary, the GDPR clearly specifies that, regarding territorial scope, it is applicable to the follows:<sup>3</sup>

---

<sup>1</sup> Available at <https://gdpr-info.eu/>

<sup>2</sup> Article 2 of the GDPR.

<sup>3</sup> Article 3 of the GDPR.

1.4.1. the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not (the establishment criterion);

1.4.2. the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to purposes of providing goods and services, or monitoring the behavior of EU data subjects (the targeting criterion); and

1.4.3. the processing of personal data by a controller not established in the Union but the GDPR is still applied by virtue of public international law.

1.5. While it is clear that entities having establishments in the territory of Vietnam are subject to the Draft Decree, it remains unclear to what extent overseas entities would be treated likewise. Before the Draft Decree, there are other documents that have touched on this issue. In particular:

1.5.1. Under Article 26.3 of the Law on Cybersecurity 2018,<sup>4</sup> overseas providers of telecommunications services, internet services and value-added services in Vietnam cyberspace that collect, analyze or process personal data or data about relationships of users or data *generated by users in Vietnam* must retain such data for a specific period of time; and such overseas providers must incorporate a branch or representative office in Vietnam; and

1.5.2. Under Article 22.1 of Decree 72/2013,<sup>5</sup> overseas providers of public information across the border and which *have users from Vietnam or can be assessed from Vietnam*, must comply with relevant Vietnamese laws. Cross-border public information provision is defined as the activity where an overseas entity uses electronic information sites, social networking sites, online applications, search services and other online equivalents in order to provide public information accessed or used by both an entity and an individual in Vietnam.<sup>6</sup>

1.6. It appears that the above provisions do not take into account the “targeting criterion”<sup>7</sup> of data processing. That said, it is not clear whether the

---

<sup>4</sup> Law on Cybersecurity of the National Assembly dated 12 June 2018 (**Law on Cybersecurity 2018**).

<sup>5</sup> Decree 72 of the Government dated 15 July 2013 on the management, provision, and use of Internet services and online information (**Decree 72/2013**).

<sup>6</sup> Article 2.1 of Circular 38 of the MIC dated 26 December 2016 specifying cross-border provision of public information (**Circular 38/2016**).

<sup>7</sup> See 1.4.2.

processing of overseas entities who do not *intend* to offer goods and services to the data subject in Vietnam would be subject to the Draft Decree. For example, a Japanese company sells goods on its website. This company does not intend to sell goods to Vietnamese residents, which is evidenced by the fact that its website is available in Japanese only, the available payment currency does not include Vietnam Dong and the method to ship the goods from Japan to Vietnam is not specified on its website. It is noteworthy that the GDPR does not cover the case where the offer of goods or services is not directed at a person in the Union.<sup>8</sup>

## **2. The notion of personal data**

2.1. At a glance, both the Draft Decree and the GDPR promulgate that information is regarded as personal data if it relates to an identified natural person or can be used to identify a natural person.<sup>9</sup> It is reasonable that the definition of personal data is often drafted in a broad manner in order to protect an individual's privacy. However, since Vietnam is a civil law country, a broad definition with no further official guidelines from the authorities might cause ambiguity for one to apply.

2.2. The following points can be drawn from the guidelines to the GDPR:<sup>10</sup>

2.2.1. Whether the information in question is identifiable should be evaluated from the perspective of third parties, rather than just the perspective of the party processing personal information (the objective approach);

2.2.2. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments; and

2.2.3. The GDPR took a risk-based approach, this means that where there is a reasonable risk of identification, data must treat such data as personal data.

---

<sup>8</sup> Guidelines 3/2018 on the territorial scope of the GDPR, pages 16 – 18.

<sup>9</sup> Article 2.1 of the Draft Decree; Article 4.1 of the GDPR.

<sup>10</sup> Recital 26 to the GDPR.

### 3. Parties involved in the processing of data

#### Overview

3.1. The table below summarizes definitions of parties involved in the processing of data under the Draft Decree and the GDPR.

	Draft Decree	GDPR
Data controller	3.1.1. The Draft Decree uses the term “personal data processor” interchangeably for both the data controller and the data processor. The personal data processor under the Draft Decree is defined as the person that processes personal data. <sup>11</sup>	3.1.2. The person who, alone or jointly with others, determines the purposes and means of the processing of personal data. <sup>12</sup> 3.1.3. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. <sup>13</sup>
Data processor		3.1.4. The person who processes personal data on behalf of the controller. <sup>14</sup>
Third party	3.1.5. The person, other than the personal data processor and the data subject, is authorized to process personal data. <sup>15</sup> 3.1.6. An employee of the data processor can fall into this group.	3.1.7. The person other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, is authorised to process personal data. <sup>16</sup>
The recipient	3.1.8. Not provided	3.1.9. The person to whom the personal data are disclosed, whether a third party or not. <sup>17</sup>

<sup>11</sup> Article 2.8 of the Draft Decree.

<sup>12</sup> Article 4.7 of the GDPR.

<sup>13</sup> Article 26.1 of the GDPR.

<sup>14</sup> Article 4.8 of the GDPR.

<sup>15</sup> Article 2.9 of the Draft Decree.

<sup>16</sup> Article 4.10 of the GDPR

<sup>17</sup> Article 4.9 of the GDPR.

*Data controller, joint controller and data processor*

3.2. One of the key difference between the Draft Decree and the GDPR is that the latter clearly allocates responsibilities among parties involved in the processing of data. For example,

3.3. Regarding the relationship between the controller and the processor, the Draft Decree requires that the controller must be responsible that the processing of data, either conducted by itself or by the processor acted on its behalf, complies with laws. The agreement between the controller and the processor must contain some compulsory provisions.<sup>18</sup>

3.4. Regarding the relationship among joint controllers, joint controllers are required to have a transparent arrangement that sets out the agreed roles and responsibilities for complying with the GDPR. The essence of the arrangement must be made available to the data subject.<sup>19</sup>

#### **4. Harmonization with other legislations**

4.1. Before the Draft Decree, there are other regulations that have already dealt with personal data. Since these regulations are fragmented, it is expected that the Draft Decree would act as comprehensive legislation. However, there are some issues that the Draft Decree fails to address. For example,

4.1.1. It is not clear how the Draft Decree address the processing of personal data which has already been made public. The Draft Decree does not directly address this issue. Instead, it is regulated that obtaining consent from the data subject is not required where other legislation allows so.<sup>20</sup> Under Article 70.4(a) of Decree 52/2014,<sup>21</sup> collecting personal information which has already been publicly disclosed on e-commerce websites are not subject to obtaining consent from such individual. However, this article is applied to information on e-commerce websites only. It is noteworthy that under the GDPR, while one can collect public personal data without obtaining further consent, he/she must inform the data subject his/her intention to process their data.<sup>22</sup>

---

<sup>18</sup> Article 28 of the GDPR.

<sup>19</sup> Article 26 of the GDPR.

<sup>20</sup> Article 10.1(a) of the Draft Decree.

<sup>21</sup> Decree 52 of the Government dated 16 May 2013 on e-commerce (**Decree 52/2013**).

<sup>22</sup> Article 14 of the GDPR.

4.1.2. It is not clear how the processing of personal data conducted by credit institutions is addressed in the Draft Decree. A credit institution when processing financial information of its customers might have to obtain approval from the PDPC (as defined at 5.2).<sup>23</sup> This requirement might cause cumbersome to the business of credit institutions.

## **5. Other notable points**

5.1. *Principles of processing personal data.* The Draft Decree introduces principles of processing personal data as follows:<sup>24</sup>

5.1.1. Principle of the lawfulness of processing. Personal data is only collected in case of necessity as prescribed by law;

5.1.2. Principle of purpose limitation. Personal data is only processed in accordance with the registered purpose, declared about processing personal information;

5.1.3. Principle of minimalism: Personal data is collected only to the extent necessary to achieve the defined purpose;

5.1.4. Principle of limited use: Personal data is only used with the consent of the data subject or with the permission of the competent authority in accordance with the law;

5.1.5. Principle of accuracy: Personal data must be updated and complete to ensure data processing purposes;

5.1.6. Principle of security: Personal data protection measures are applied during the processing of personal data;

5.1.7. Personal principle: Data subjects know and receive notifications about their activities related to the processing of personal data; and

5.1.8. Privacy principle: Personal data must be kept confidential during data processing.

5.2. *Personal Data Protection Committee.* Under the Draft Decree, the Personal Data Protection Committee (**PDPC**) will be incorporated. The PDPC is in charge of, among others, assessing applications for processing sensitive personal data

---

<sup>23</sup> Articles 2.3(h) and 20.1 of the Draft Decree.

<sup>24</sup> Article 3 of the Draft Decree.

and cross-border transferring of personal data.<sup>25</sup>

5.3. *Personal data of children.* Processing children information is subject to stricter requirements.<sup>26</sup>

5.4. *Cross-border transfer of personal data.* The following requirements must be met when transferring personal data outside of Vietnam:<sup>27</sup>

5.4.1. The data subject consents to the transfer;

5.4.2. Original data is stored in Vietnam;

5.4.3. The country/territory where the data is transferred to has regulations on personal data protection at an equal or higher level than those under the Draft Decree; and

5.4.4. The PDPC approves such transfer.

- *End of documents* -

---

<sup>25</sup> Article 24.16 of the Draft Decree.

<sup>26</sup> Article of the Draft Decree.

<sup>27</sup> Article 21.1 of the Draft Decree.