ARTICLE NO.2
A DEEPER DIVE INTO PERSONAL DATA PROCESSING UNDER THE VIETNAM DRAFT LAW ON PERSONAL DATA PROTECTION AND GDPR

Abstract: *This Article compares Draft Law on personal data protection ("**Draft Law**") with the EU General Data Protection Regulation ("**GDPR**"). It highlights the progress of Draft Law in enhancing privacy protections but notes its limitations compared to the GDPR. Despite sharing some basic principles on the purpose limitation, data minimization and accountability, the Draft Law has a narrower scope, less clarity on profiling, and uncertainty about de-identification of personal data. These differences highlight the need for further refinement to align with international standards and ensure effective data protection once enacted.*

Keywords: #PersonalData #GDPRvsDraft Law #DataPrivacyLaw #LegalFramework #GDPRCompliance

While both the GDPR and the Draft Law share common principles such as purpose limitation, data minimization, and accountability, they differ significantly in several areas. Firstly, the Draft Law has limited the implications and scope of processing personal data. Unlike the GDPR, which provides a comprehensive framework covering a wide range of data processing activities, the Draft Law's scope is narrower and less detailed. Secondly, the Draft Law appears to misunderstand and may not fully capture the nuances of the concept of "profiling", which is explicitly defined and regulated under the GDPR to ensure robust protections for individuals against automated decision-making. Lastly, while the GDPR clearly distinguishes between anonymized and pseudonymized data, the Draft Law does not provide the same level of clarity, leading to potential confusion about the regulatory obligations for de-identified data. These differences highlight the need for further refinement of the Draft Law to align more closely with international standards and ensure comprehensive data protection once it is enacted.

1. The Draft Law Has Limited The Implications And Scope Of Processing Personal Data

The GDPR, enacted as Regulation (EU) 2016/679, provides a broad and inclusive definition of "processing" in Article 4(2) of the GDPR:

> "*Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*.".

Pursuant to Recital 15 on technology neutrality of the GDPR, the legislators aimed to prevent circumvention and ensure the regulation's applicability regardless of technological changes. The implication of technology neutrality covers:

(i) Fully automated processes (e.g., using computers, smartphones, webcams, drones).

(ii) Partially automated processes (manual processing) involving human intervention, if the personal data are contained or are intended to be contained in a ***filing system***. It should be noted that a filing system is not necessarily be an electronic system or a digital system. In the case of C-25/17 Jehovan todistajat[1] (Jehovah's Witnesses), a religious community collected personal data during door-to-door preaching to help remember information for future visits. The Court of Justice of the European Union ruled that this practice constitutes a ***filing system*** because the data are collected as ***memory aid for later use***. This practice demonstrates that even non-digital, manual processing or memorizing personal data can qualify as a ***filing system*** and therefore subject to the regulations of the GDPR.

The inclusion of manual processing within the scope of the GDPR is particularly important in ensuring that traditional data-handling methods—such as paper records, manual filing systems, or non-automated data entry—are not exempt from data protection obligations. As such, even if data is processed manually by a human, if it can be linked to an individual or used to identify that individual, the processing is still subject to the requirements of the GDPR, including principles of fairness, transparency, and data minimization. The GDPR aims to maintain a flexible framework capable of addressing the diverse methods of processing data across different sectors and industries.

Meanwhile, Vietnam's Draft Law on Personal Data Protection similarly adopts an extensive approach to defining data processing. The Draft Law stipulates that "data processing" includes "*activities such as collection, recording, analysis, confirmation, storage, modification, disclosure, combination, access, retrieval, encryption, decryption, copying, sharing, transmission, provision, transfer, deletion, or destruction of personal data*." This definition spans the entire lifecycle of personal data handling, from initial collection to final destruction.

Unlike the GDPR, the Draft Law explicitly lists activities such as "analysis," "confirmation," "encryption," and "decryption," indicating a focus on specific modern data practices. However, the Draft Law does not clarify whether partially automated processes (or manual processing) are governed. Given that "personal data" under the Draft Law is defined as "electronic information", it can be concluded that the nature of the Draft Law does not cover manual processing of personal data, henceforth. This critical omission may result in a less defined scope of processing under the Draft Law compared to the GDPR.

2. The Draft Law Is Misunderstanding The Concept of "Profiling"

The GDPR provides a comprehensive and explicit framework for profiling, ensuring that all forms of automated processing are regulated and that individuals' rights are protected.

[1] https://gdprhub.eu/index.php?title=CJEU_-_C-25/17_-_Jehovan_todistajat

In contrast, the Draft Law only governs the practices of profiling in deployment of AI systems.

The GDPR explicitly defines profiling in Article 4(4) as any form of "automated processing" of personal data used to evaluate personal aspects of an individual. Profiling under the GDPR is subject to strict regulations, particularly when it involves automated decision-making that significantly affects individuals. Article 22 of the GDPR grants individuals the right not to be subject to decisions based solely on automated processing, including profiling, unless specific conditions are met, such as explicit consent or contractual necessity. Additionally, Recital 71 of the GDPR emphasizes the need for safeguards, including the right to obtain human intervention, express a viewpoint, and contest decisions. Such clear definition allows for targeted regulation of profiling activities, ensuring that individual's rights are protected in various contexts, including but not limited to marketing, credit scoring, and employment decisions.

Meanwhile, the Draft Law provides a similar definition of "profiling", i.e. "*automated processing of personal data is a form of data processing carried out by electronic means to evaluate, analyze, and predict the activities of a specific individual, such as habits, preferences, reliability, behavior, location, trends, capabilities, and other aspects*"[2]. However, the term "automated processing of personal data" appears only once in the section on AI systems, which means other forms of profiling, such as those used in marketing or analytics, are less regulated or potentially forgotten.

It should also be noted that "profiling" under the GDPR does not exclude human intervention. The definition of "profiling" refers to "automated processing", but "processing" itself can involve both automated and non-automated means. This implies that the GDPR acknowledges semi-automated processes where human intervention occurs, such as manually entering personal data into a digital system. Therefore, if humans process data according to a predefined procedure but still involve technology, it can be considered part of automated processing and subject to profiling regulations[3].

3. The Draft Law Is Uncertain About De-identification of Personal Data

The Draft Law defines the "de-identification of personal data as the process of *anonymizing* or *removing identifying content or replacing* it with fictitious names or codes to create new data that cannot identify a specific individual"[4]. The GDPR, on the other hand, excluded the processing of anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable[5]. Consequently, it remains unclear whether anonymized data controlled by the data controller is subject to the regulatory obligations under the Draft Law or not.

[2] Article 2.(23) of the Draft Law;
[3] Recital 71 of the GDPR;
[4] Article 2.(25) of the Draft Law;
[5] Recital 26 of the GDPR;

Meanwhile, Article 4(5) of the GDPR defines "*pseudonymisation as the processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without additional information, provided that such information is kept separately and is subject to technical and organisational measures to ensure that the data are not attributed to an identified or identifiable natural person*". It appears that the Draft Law is attempting to mimic the term "pseudonymisation" but has inadvertently included "anonymization" activities within the term "de-identification." If this is the case, adjustments should be made to clearly state that anonymized data should not fall under the regulations of the Draft Law and should be exempt from regulatory obligations.

Additionally, the regulation on de-identification of personal data is only used once in the context of personal data protection in financial, banking, credit, and credit information activities. It remains unclear how the Draft Law will apply this regulation once it is officially enacted.

4. Purpose Limitation, Data Minimization, and Accountability

The principles of purpose limitation, data minimization, and accountability are foundation concepts in data protection law, and they are designed to ensure that personal data is processed in a lawful, transparent, and ethical manner.

a. Purpose Limitation

The principle of purpose limitation requires that personal data be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes[6].

Furthermore, Article 6(1) of the GDPR outlines the lawful bases for processing personal data, with each processing purpose needing to align with one of these bases (e.g. consent, contractual necessity, or compliance with a legal obligation). Then, the GDPR sets out clear guidelines on what constitutes compatible and legitimate purposes. For instance, the Recital 50 of the GDPR clarifies that additional processing for purposes such as public-interest archiving, scientific or historical research, or statistical analysis, as specified in Article 89(1) of the GDPR, is not considered incompatible with the initial purposes[7]. This exception supports flexibility within the regulatory framework, allowing certain secondary uses of data when they serve significant public or scientific interests without compromising the data subject's rights.

By comparison, The Draft Law enforces a stricter interpretation of purpose limitation. Similar to the GDPR, it mandates that data be processed only for the initially specified purposes[8], but it offers fewer exceptions for secondary processing and impose the burden

[6] Article 5(1)(b) of the GDPR;
[7] Article 89(1) of the GDPR "*Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes*."
[8] Article 3(3) of the Draft Law.

of proof on the controller/processor in such cases (e.g. health emergency, national security and defense, epidemic, etc.). For example, if the GDPR allow for compatible scientific processing, the Draft Law restricts such use unless the data subject provides additional explicit consent.

b. Data minimization

Both the GDPR and the Draft Law require data minimization, meaning that personal data should be adequate, relevant, and limited to what is necessary for the purpose. However, the specific implementation and enforcement of these requirements may vary.

In its Article 5(1)(c)[9], the GDPR firmly establishes this obligation and requires data controllers to limit data collection to avoid excesses, backed by strong enforcement mechanisms, including high fines for non-compliance. The Draft Law similarly incorporates data minimization, though its approach is less comprehensive than the GDPR's. Article 3(4) of the Draft Law provides that "*personal data shall only be collected to the minimum necessary for the purpose of processing.*" This definition mirrors the GDPR's intent to restrict data processing to what is essential. However, the Draft Law provides little additional guidance on how this principle should be applied, leaving room for interpretation by the controller(s) and the processor(s).

c. Accountability

The legal frameworks of the GDPR and the Draft Law both impose liability obligations on controllers and processors by forcing the controller(s) and the processor(s) to demonstrate their compliance with data protection principles, i.e. lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality. Nevertheless, if the GDPR is literally silent on the selling of personal data the Draft Law imposes a stricter rule on the controller(s) and the processor(s) by prohibiting the buying and selling of personal data.

The GDPR places a strong emphasis on accountability defined in its Article 5(2)[10], which translates into the obligation to implement appropriate technical and organizational measures, such as data protection impact assessments[11] ("**DPIA**") and keeping a register of processing activities[12]. Unlike the GDPR, the Draft Law does not explicitly define "accountability" and does not directly instruct the controller(s) and the processor(s) on how to demonstrate their compliance. Although the DPIA is applicable, the controller(s) and the processor(s) are also required to keep paper record or electronic record of their processing activities, the lack of explicit guidance and rule on how to demonstrate compliance could

[9] Article 5(1)(c) of the GDPR "*Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')*";
[10] Article 5(2) of the GDPR "*The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')*".
[11] Article 35 of the GDPR
[12] Article 30 of the GDPR

significantly impact the dissemination, education, and awareness of the Draft Law upon its enforcement.

The GDPR also provides for significant penalties for non-compliance, up to €20 millions or 4% of worldwide sales, to ensure a high level of enforcement. On the other hand, Article 4 of the Draft Law[13] references administrative or criminal penalties for violations, but it offers no specifics on the nature or scale of the violations. Currently, the regulatory framework in Vietnam for penalties related to personal data protection is fragmented across various laws and decrees. For instance, Decree 15/2020/ND-CP governs administrative sanctions in the sectors of postal services, telecommunications, radio frequencies, information technology, and electronic transactions[14]; Decree 24/2025/ND-CP addresses administrative sanctions for breaches involving consumers' sensitive personal data[15]; and the Criminal Code 2015 criminalizes the illegal use of information on computer or telecommunications networks[16]. It is widely anticipated that as Vietnam's data protection regime matures, forthcoming regulations will establish a clearer and more comprehensive penalty structure.

[13] Article 4 of the Draft Law "*Agencies, organizations and individuals that commit violation of the regulations on personal data protection, depending on the severity, may be subject to disciplinary, administrative or criminal penalty in accordance with applicable regulations*."
[14] Articles 84-86, 100-106 of Decree 15/2020/ND-CP
[15] Article 46.3 of Decree 24/2025/ND-CP
[16] Article 288 of Criminal Code 2015

AUTHOR(S)

TRAN DAI PHONG
Associate
E: phong.tran@asialegal.vn

HOANG KHAC VINH
Legal Assistant
E: vinh.hoang@asialegal.vn

CONTACT:

Telephone:
(+84) 24 2269 3399

Hotline:
(+84) 84 400 8484

Email:
info@asialegal.vn

Website:
www.asialegal.vn

Headquarter (Hanoi)
15th Floor, HT Building, No. 80 Duy Tan, Cau Giay District, Hanoi, Vietnam.

ABOUT ASIA LEGAL:

Asia Legal is one of the reputable business law firms in Vietnam. At Asia Legal, our commitment lies not only in providing conventional legal services but also in delivering tailored legal solutions that align with the business requirements of our clients. Our approach is founded upon an in-depth comprehension of Vietnamese legislation and a thorough understanding of the unique commercial landscape each client operates within.

To ensure the provision of high-quality service to our clients, we focus our endeavors exclusively on catering developing deeply to the service segments as follow:

- Mergers & Acquisitions
- Dispute Resolution
- Foreign Investment
- International Trade
- Energy & Natural Resources
- Real Estate & Construction
- Labor & Employment
- Data Privacy
- Intellectual Property

SCAN QR CODE TO JOIN US