ARTICLE NO.3
JOINT CONTROL OF PERSONAL DATA UNDER THE DRAFT LAW ON PERSONAL DATA PROTECTION AND GENERAL DATA PROTECTION REGULATION

***Abstract**: In today's interconnected digital landscape, personal data protection has become a cornerstone of privacy rights, with the concept of joint control emerging as a pivotal issue. Joint control arises when multiple entities collaborate to process personal data, necessitating clear legal frameworks to ensure accountability and safeguard data subjects. The European Union's General Data Protection Regulation **("GDPR")** offers a robust model for addressing joint controllers, setting a global standard. By contrast, Vietnam's Draft Law on Personal Data Protection **("Draft Law")**, issued on March 10, 2025, remains silent on this critical aspect, raising questions about its adequacy in a data-driven era. This article provides a comprehensive comparison of how the GDPR and the Draft Law address joint control, analyzing the definitions of entities involved in data processing, the GDPR's regulation of joint controllers, relevant case studies, the implications of the Draft Law's omission, and recommendations for improvement.*
Keywords: #PersonalData #GDPRvsDraft Law #DataPrivacyLaw #LegalFramework #GDPRCompliance #JointController

1. Definitions of Entities Involved in Data Processing: A Comparative Analysis

A clear understanding of the entities involved in data processing is essential to delineating responsibilities, particularly in the context of joint control. The GDPR and the Draft Law define several key roles, with notable similarities and differences that shape their approaches to data governance.

<table>
<tr><th>Definitions</th><th>GDPR</th><th>Draft Law</th></tr>
<tr><td rowspan="2">Controller</td><td>a natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of processing personal data.</td><td>as an organization or individual determining the purpose and means of processing personal data.</td></tr>
<tr><td colspan="2">This alignment underscores a shared emphasis on decision-making authority as the hallmark of a controller, whether acting independently or collaboratively</td></tr>
<tr><td rowspan="2">Processor</td><td>is an entity that processes personal data on behalf of the controller[1], typically under explicit instructions, such as IT service providers or cloud storage companies.</td><td>Personal Data Processor ("PDP") as an organization or individual processing data on behalf of the Personal Data Controller ("PDC").</td></tr>
<tr><td colspan="2">The Draft Law mirrors the definitions from GDPR reflecting a consistent delineation of operational roles across both frameworks.</td></tr>
</table>

[1] Article 4(8) of GDPR.

Third party	any entity—other than the data subject, controller, processor, or their authorized agents—that may access or process personal data outside the primary controller-processor relationship[2].	entities beyond the data subject, PDC, PDP, or Personal Data Controller and Processor ("**PDCP**") permitted to process personal data[3].
	Both definitions parallelly identify third parties as entities beyond core roles, emphasizing similar scopes for external data processors.	

Unique to the Draft Law is the **PDCP**, an entity that both determines the **purposes** and **means** of processing and directly processes the data. This hybrid role, absent from the GDPR, may address scenarios where a single organization manages all aspects of data handling internally, such as a company maintaining its customer database without outsourcing. However, it does not extend to multiple entities collaborating jointly, leaving a gap in the Draft Law's framework.

The GDPR explicitly recognizes **joint controllers** as a concept critical to partnerships or integrated services. Strikingly, the Draft Law lacks any equivalent provision, creating a significant omission that hinders its ability to regulate multi-entity data processing arrangements.

This comparative analysis reveals that while the Draft Law supplements the GDPR's taxonomy with the PDCP role, its failure to address joint controllers represents a shortfall. The subsequent sections explore how this gap contrasts with the GDPR's comprehensive approach and its implications for Vietnam's data protection regime.

2. GDPR's Regulation on joint controllers

The GDPR provides a detailed framework for joint controllers under Article 26, acknowledging the complexities of modern data processing where multiple entities may share decision-making authority. This provision ensures clarity, accountability, and protection for data subjects in collaborative contexts.

Joint controllers are defined as entities that jointly determine the purposes and means of processing personal data[4], such as two companies collaborating on a marketing campaign to collect customer data. Their responsibilities must be delineated through a transparent arrangement—typically a contract—specifying obligations like informing data subjects[5], facilitating data subject rights[6], and implementing security measures[7]. This

[2] Article 4(10) of GDPR.
[3] Article 2(15) of Draft Law.
[4] Article 26(1) of GDPR.
[5] Articles 13-14 of GDPR.
[6] Articles 15-22 of GDPR.
[7] Article 32 of GDPR.

arrangement ensures that compliance reflects each controller's role and relationship with the data subjects.

A key feature of this framework is its accessibility to data subjects. Regardless of the internal division of duties, individuals can exercise their rights—such as access, rectification, or erasure—against any joint controller[8]. This joint-and-several-liability approach simplifies enforcement and reinforces accountability, ensuring that data subjects are not burdened by the complexities of multi-entity arrangements. Moreover, the essence of the arrangement must be made available to data subjects, enhancing transparency about whom to contact and how their data is managed[9].

For instance, if two firms jointly launch a customer survey, one collecting data and the other analyzing it, they must establish an agreement clarifying their roles. Both remain accountable to the data subjects, aligning with the GDPR's principles of transparency and accountability while enabling collaboration.

3. Case Studies on joint controllers under GDPR

The practical application of joint controllership under the GDPR has been elucidated through landmark rulings by the **Court of Justice of the European Union (CJEU)**, offering valuable insights into its scope and implications.

In the **Facebook Fanpage Case (C-210/16, Judgment of 5 June 2018)**, a German company operated a fan page on Facebook, utilizing cookies and analytics tools provided by the platform to collect visitor data[10]. The CJEU determined that the fan page administrator was a joint controller with Facebook. Although the administrator lacked control over the technical processing tools, its decision to leverage the fan page for promotional purposes contributed to defining the purposes and means of processing. This ruling broadened joint controllership to include entities using third-party platforms, emphasizing that active participation triggers responsibility.

Similarly, the **Fashion ID Case (C-40/17, Judgment of 29 July 2019)** involved a German online retailer embedding a Facebook "Like" button on its website, enabling Facebook to collect visitor data via cookies, even without interaction[11]. The CJEU ruled that the retailer was a joint controller with Facebook for the collection and transmission of data, though its liability was confined to this initial phase, as it had no influence over Facebook's subsequent processing. This decision underscored that joint controllership can be partial, applying to specific processing stages, and highlighted the compliance risks of integrating third-party tools.

These cases demonstrate the GDPR's flexibility in addressing joint controllership in digital contexts. They have heightened awareness among businesses about the

[8] Article 26(3) of GDPR.
[9] Article 26(2) of GDPR.
[10] C-210/16 - Wirtschaftsakademie Schleswig-Holstein, Court of Justice of the European Union, 05/06/2018
[11] C-40/17 - Fashion ID, Court of Justice of the European Union, 29/07/2019

compliance implications of using third-party tools, prompting clearer contractual arrangements and transparency measures.

4. Implications of the Draft Law's silence on joint controllers

The Draft Law's omission of provisions for joint controllers presents significant challenges to data protection, compliance, and accountability in Vietnam, with widespread implications.

The Draft Law's failure to address joint controllers introduces significant challenges for data protection, compliance, and accountability in Vietnam, with far-reaching consequences.

Without a joint controllership framework, responsibility becomes ambiguous. In scenarios where multiple entities—such as two firms collaborating on a shared service—jointly decide on the purposes and methods of data processing, the Draft Law fails to offer guidance on allocating duties like notifying data subjects or responding to rights requests. Consequently, each controller operates independently, disregarding the interconnected nature of their activities. This fragmented approach complicates the understanding of actual data processing flows and leads to redundant administrative efforts. For example, both entities may separately notify data subjects or duplicate compliance procedures, amplifying inefficiency and increasing the risk of errors.

The challenges extend to data subjects who face barriers in exercising their rights. Under the GDPR, individuals can address any joint controller for redress, simplifying access to remedies. Vietnam's absence of such a mechanism makes identifying the responsible entity in complex processing chains difficult, potentially undermining protections like data access and erasure.

For organizations, compliance burdens rise without coordinated joint controllership. Each entity may independently fulfill obligations, such as obtaining consent or conducting data protection impact assessments, leading to duplicative efforts and higher costs—particularly for collaborative projects.

This gap also creates significant accountability issues. The GDPR's joint-and-several-liability framework ensures comprehensive redress, with internal settlements distributing liabilities. In Vietnam, however, entities might only be accountable for their specific actions, leaving gaps where no party assumes full responsibility for breaches or damages. This is especially problematic when entities have varying purposes, methods, or policies. For instance, if two firms process the same data but apply different security standards, the lack of a unified framework leads to inconsistencies that confuse data subjects and complicate regulatory enforcement.

Additionally, Vietnam risks misalignment with international standards. Multinational firms accustomed to GDPR-compliant joint controllership may encounter operational challenges in Vietnam, hindering cross-border data flows and integration into the global digital

economy. The lack of a framework also inhibits responsible data sharing, which could stifle innovation in industries like technology and research.

Although the PDCP role is innovative, it does not address these issues. It applies to a single entity performing dual functions, rather than multiple entities working together. As a result, two Vietnamese firms jointly processing data would be treated as separate PDCs, resulting in overlapping efforts instead of streamlined collaboration

5. Recommendations for the Draft Law

To address these deficiencies, the Draft Law should incorporate a provision on joint controllers, drawing inspiration from the GDPR. We propose the following tailored text:

"Where two or more controllers jointly determine the purposes and means of processing personal data, they shall be deemed joint controllers. They must transparently define their respective obligations to ensure compliance with this Law and protect data subjects' rights, potentially designating a single point of contact. The core elements of this arrangement shall be accessible to data subjects, who may exercise their rights against any joint controller."

This provision would establish clear guidelines for collaboration, prevent misuse, and reduce privacy risks by ensuring accountability and transparency. It aligns with broader data protection principles, fostering trust among individuals and organizations in Vietnam's data ecosystem.

AUTHOR(S)

NGUYỄN TRỌNG HIẾU
Senior Associate
E: hieu.nguyen@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