



March 17, 2025

GLOBAL DATA ALLIANCE COMMENTS ON THE DRAFT DECREE AND DRAFT DECISION TO IMPLEMENT THE DATA LAW

The Global Data Alliance (**GDA**) thanks the Ministry of Public Security (**MPS**) for the opportunity to comment on the draft decree on detailed regulations on a number of articles and measures to implement the Data Law (**Draft Decree**)¹ and on the Draft Decision promulgating a list of important and core data (**Draft Decision**).²

The GDA is a cross-industry coalition of companies, headquartered in different regions of the world, that are committed to high standards of data privacy and security. The GDA supports policies that help instill trust in the digital economy without imposing undue cross-border data restrictions or localization requirements that undermine data security, cybersecurity, innovation, economic development, and international trade. Given the GDA's focus on cross-border data, we comment specifically on the cross-border data aspects in the development of the Draft Decree and Draft Decision to implement the Data Law.

We hope that these suggestions will help the MPS to refine the Draft Decree and Draft Decision. Please consider the GDA to be a resource for MPS as you develop a comprehensive and robust data governance framework that is interoperable with international best practices, especially in relation to cross-border data transfers, harmonizes with Vietnam's personal data protection regulations, and supports the growth of a vibrant and innovative digital economy.

Roles and Responsibilities of Data Owners and Data Administrators

While the Data Law defines the data administrator and data owner within Articles 3.13 and 3.14 respectively, it does not show how the relationship between the data administrator and data owner should be governed, for example, through a contractual arrangement or otherwise. Throughout the Data Law and Draft Decree, many responsibilities fall on the data administrator despite the data owner being the party with the "right to decide on the formulation, development, protection, administration, processing, use and exchange of value of data in its possession." In

¹ See public consultation by MPS on the Draft Decree, at <https://bocongan.gov.vn/pbgdpl/van-ban-du-thao/du-thao-nghi-dinh-quy-dinh-chi-tiet-va-bien-phap-thi-hanh-luat-du-lieu-516.html>.

² See public consultation by MPS on the Draft Decision, at <https://bocongan.gov.vn/pbgdpl/van-ban-du-thao/du-thao-quyet-dinh-ban-hanh-danh-muc-du-lieu-quan-trong-du-lieu-cot-loi-518.html>.

contrast, the data administrator is the party that “develops, manages, operates and exploits data at the request of the data owner.”

Since the data owners decide how data is formulated, developed, protected, administered, processed, used and exchanged, they should have primary responsibility for satisfying the obligations on the data. Data administrators, which act upon instructions from the data owners on how the data should be formulated, developed, protected, administered, processed, used and exchanged, should employ reasonable and appropriate security measures to prevent unauthorized access, use, or disclosure of the data and should be responsible for following instructions from the data owners according to contractual arrangements between the two parties. This is similar to the controller-processor distinction in personal data protection laws, whereby the personal data controllers decide how and why to collect and use personal data and the personal data processor processes personal data on behalf of the personal data controller.³

Recommendation: The GDA recommends that obligations affecting how and why data is collected and used be placed on the data owners, rather than on data administrators. This reflects the different roles of these different entities. For instance, the data owner should be the party responsible for the quality and authentication of data within Articles 9.1(d), 9.2, and 9.4 of the Draft Decree, because it is the party deciding how and why to collect that data. Similarly, the data owner is the party best placed to carry out the self-assessment of risks prior to the transfer of data overseas and should be responsible for doing so within Articles 12.2, 12.6, and 12.7 of the Draft Decree. Further, Article 15 does not specify the entity responsible for managing risks arising from data processing. We recommend that the data owner should be the responsible party, and that the responsibilities of the data administrator should be specified in contractual terms between the data owner and the data administrator. Similarly, Articles 17.2 and 18 place responsibilities on the data administrator that are inconsistent with their role in processing data on behalf of other entities; these include obligations to classify data and identify Core and Important Data, and to manage the data protection process. Accordingly, the data owner should be the responsible party, and any obligations placed on data administrators should be limited to assisting the data owners in carrying out this work on behalf of the data owner.

Recommendation: Article 17.1 of the Draft Decree, where “[t]he data owner and data administrator are state agencies responsible for the security of data processing activities, implementing hierarchical protection for all types of data,” could be read to mean that only state agencies can be data owners and data administrators. If it is indeed the policy intent that only state agencies can be data owners or data administrators, the Draft Decree should state that explicitly. It should then make clear any obligations, if any, that would apply to non-state agencies, organizations and individuals that are currently under scope within Article 2 of the Draft Decree.

³ See The Global Standard: Distinguishing Between Controllers and Processors in Privacy Legislation, available in English and Vietnamese at <https://www.bsa.org/policy-filings/the-global-standard-distinguishing-between-controllers-and-processors-in-privacy-legislation>.

Core Data

We appreciate that Article 4 of the Draft Decree provides broad categories of data considered Core Data that appear to be solely data that is usually held only by government or state agencies.

Recommendation: To avoid confusion, we recommend that the MPS make clear that Core Data will only cover specific subsets of data that reside within the public sector, and that private sector data should be explicitly excluded from Core Data. Further, if data that is considered Core Data is transferred from state agencies to non-state agencies, the state agencies should explicitly inform the non-state agency that Core Data is transferred, with specific instructions on how to deal with it.

Recommendation: We recommend deleting Article 1.21 in the Draft Decision, i.e., data on cross-border banking transactions (from 50,000 transactions or more) should be removed to confine Core Data to public sector data. The classification of data as core or important should be determined by its characteristics rather than its volume. For instance, if a cross-border banking transaction is not considered core data, increasing its frequency to 50,000 does not make it any more impactful to national security.

Recommendation: While we appreciate that Article 1 of the Draft Decision provides a detailed list of the data considered Core Data, the MPS should state that the list is exhaustive and does not include further categories of data. This will provide certainty to the various parties involved.

Important Data

The criteria for Important Data under Articles 3.3 and 3.4 of the Draft Decree are overly broad. For example, data that affects “economic development, macroeconomics, national economic lifeline, and infrastructure of important economic sectors” and data that affects “the life, health, honor, dignity, property, rights and legitimate interests of agencies, organizations and individuals” could potentially include nearly all data that a company uses to run its business, whether or not it is truly important or critical to national security or public security. A broad classification of important data risks over-inclusiveness, creating burdensome compliance obligations for businesses without achieving Vietnam’s intended policy outcomes. This will stifle innovation and restrict business operations, hindering Vietnam’s digital and economic development.

Recommendation: We recommend deleting Articles 3.3 and 3.4. Instead, Article 3 of the Draft Decree should state that the list of data types will be specified within the Draft Decision.

Recommendation: Remove data classes involving personal data from the list of Important Data specified in the Draft Decision as personal data is already regulated under existing personal data protection legislations. Specifically, we recommend deleting Articles 2.6(c), 2.6(d), 2.8(a), 2.8(c), 2.8(d), 2.15(d), and 2.16 since they all involve personal data and are more appropriately regulated under the Personal Data Protection Law (**PDP Law**) or Personal Data Protection Decree (**PDP Decree**).

Some of the data types listed in Article 2 of the Draft Decision are overly broad. For example, Article 2.15(c) refers to data related to the construction and deployment of resources and security of important networks and information systems.

Recommendation: MPS should specify the factors that make a network or information system “important” or notify the entities that hold such data that is considered Important Data. Further, MPS should restrict the types of data considered Important Data to only the data that directly implicates national security.

Cross-border data transfers

The Data Law and its implementing decrees and decisions should enable and encourage global data transfers, which underpin the global economy and are vital to the security of networks and information systems. Indeed, the Report on the Draft Decree outlines the policy objectives of promoting “the digital transformation of the Party and the State,” “integrating Vietnam with countries in the region and the world,” “completing the legal corridor to promote digital transformation,” and “developing digital government, digital economy, and digital society.”⁴ We further note Vietnam’s interest and engagement in the Global Cross Border Privacy Rules (CBPR) Forum, recognizing that cross-border data transfers are an important aspect of Vietnam’s growing digital economy. However, we are concerned that the broad definitions of Core and Important Data, together with onerous requirements for assessment, reporting and requesting approval from the authorities, are barriers to cross-border data transfers.

Organizations that transfer data globally should implement procedures to ensure the data transferred outside of the country continues to be protected. Where differences exist among data protection regimes, governments should create tools to bridge those gaps in ways that both protect privacy and facilitate global data transfers. Data governance frameworks should not impose data localization requirements for either the public or private sectors, because such requirements can frustrate efforts to implement effective security measures, protect data, and defend critical networks, just as they can impede business innovation and limit services available to consumers.

As noted in our prior submissions, restrictions on cross-border transfers have a chilling effect on the local economy as they restrict domestic enterprises and other organizations from fully benefiting from cutting edge technology and services available in the global marketplace. For instance, restrictions on cross-border data transfers may prevent domestic companies, including small and medium-sized enterprises (SMEs) and larger organizations such as hospitals, airlines, and banks, from using world leading information technology and cloud computing solutions from service providers that offer their services from outside of Vietnam. Such services frequently provide best-in-class security capabilities. Domestic companies subject to data transfer restrictions are likely to find it difficult to access such services, reducing their competitiveness, especially internationally, and exposing them to greater data security risks. Restrictions on international data transfers are also resource-intensive for government authorities to manage.

⁴ See Paragraph II.1(b) and (d) in the Report on the Draft Decree.

It is inadvisable to restrict data transfers for “important data” or “core data” categories that could sweep broadly enough to include any type of personal and non-personal data, proprietary information, or machine-to-machine data etc., commonplace in everyday business operations. Such data is unlike the type of highly sensitive government data that may actually implicate national security concerns. Accordingly, we urge Vietnam to avoid the imposition of unnecessary or arbitrary restrictions on cross-border data transfers, given Vietnam’s relatively high restrictiveness score on international indices of cross-border data transfer policies.⁵ For both non-governmental data and governmental data. Vietnam’s regulatory efforts should focus on enabling cross-border data transfers in the digital economy – consistent with Vietnam’s treaty commitments under Article 12 of the WTO Agreement on E-Commerce to seek to “facilitate public access to and use of government data” – while considering a more nuanced approach towards data governance at the same time, that does not impinge its national security and public policy objectives.⁶

Recommendation: In addition to our earlier recommendation that the categories of Core and Important Data should be restricted to only those that directly implicate national security, we recommend that only data owners that are transferring Core or Important data overseas are required to conduct the self-assessment and reporting process outlined in Article 12.3-5, 9, and 10. Data owners or administrators of data that is not Core or Important Data should not be required to conduct this self-assessment and reporting process. This will be in line with the policy intent to “optimize the exploitation, share and use of data resources, ensure efficiency in digital transformation” and for Vietnam to integrate with countries in the region and the world, as stated in the Report on the Decision (see paragraphs I.2 and II.2(d)).⁷

Recommendation: Where personal data is processed, the requirements under the Draft Decree should align with those under the PDP Law or PDP Decree (as the case may be). For example, a single impact assessment should be sufficient under the Data Law and PDP Law so that there is no duplication of reporting requirements.

Transition Period

Extending the legislative timeline for the Draft Decree is crucial to ensure comprehensive stakeholder engagement and thoughtful development of the law. A rushed timeline risks overlooking critical feedback from experts, industry players, civil society, and other key stakeholders, which could lead to unintended consequences such as regulatory gaps or unnecessarily burdensome compliance requirements. Allowing more time for dialogue and collaboration will enable the creation of a more balanced and effective legal framework that aligns with global best practices while addressing Vietnam’s unique context and requirements. An extended timeline would also provide sufficient opportunity to refine and harmonize the provisions within the Data Law, the implementing Decree, and Decision with the existing Law on

⁵ See Global Data Alliance, *Cross-Border Data Policy Index* (2023), at: <https://globaldataalliance.org/resource/cross-border-data-policy-index/>

⁶ See also, BSA | The Software Alliance, *Open Data - Bridging the Data Divide* (2021), <https://www.bsa.org/files/policy-filings/061120bsaopendata.pdf>

⁷ See paragraphs I.2 and II.2(d) of the Report on the Draft Decision.

Cybersecurity and the upcoming PDP Law. This will lead to a more robust data governance regime.

Recommendation: We recommend including sufficient time for engagement with stakeholders before promulgating the Draft Decree and recommend a two-year transition period from the time the decree is enacted to the commencement of its effective date. This will allow harmonization of the various laws on data and provide organizations sufficient time to adjust their systems and processes to comply with the Data Law, the implementing Decree, and the Decision on Core and Important Data.

Conclusion

In conclusion, we respectfully recommend that Vietnam allocate roles and responsibilities of data owners and data administrators more appropriately, narrow the definitions of Core and Important Data to only data that directly implicates national security, remove onerous requirements for cross-border data transfers, and streamline requirements under the Data Law with requirements under the PDP Law. We appreciate the opportunity to share these views and hope that they will be helpful as Vietnam refines its Draft Decree and Draft Decision. Please do not hesitate to contact us with any questions regarding this submission.

Thank you for the opportunity to provide comments.

Sincerely,

Joseph P. Whitlock
Executive Director
Global Data Alliance
josephw@bsa.org