



18 November 2021

Comments On Proposed Amendments To Draft Decree On Sanctions Against Administrative Violations In the Field of Cybersecurity

Submitted electronically to the Ministry of Public Security

The Global Data Alliance (**GDA**)¹ welcomes the opportunity to provide our comments to the Ministry of Public Security (**MPS**) on the draft Decree on Sanctions against Administrative Violations in the field of Cybersecurity (**Draft Decree**). While member companies may have interests and concerns on a range of issues raised in Draft Decree, the GDA is focused on policies related to cross-border data transfers. Accordingly, this submission addresses those provisions that are relevant to cross-border data transfers.

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. Members of the GDA represent sectors as diverse as agriculture, healthcare, manufacturing, and banking — and we are united in the need to send data across international borders to provide people and their communities with the information, products, and services they need. We recognize that today's cross-border economy depends on the trust of regulators, consumers, and the general public.

The ability to transfer data, including personal data, across international borders is the lifeblood of the modern digital economy. Indeed, the ability to send data across borders is vital not just to businesses, but also to consumers and workers. A forward-leaning policy on cross-border data transfers, which is interoperable with international frameworks, is a particularly effective tool which can help policymakers drive innovation, enhance quality of life, increase employment, and create other economic and societal benefits.

The GDA has a significant interest in Viet Nam's Law on Cyber Security (**LOCS**) and its corresponding draft decrees, such as the draft Decree on Personal Data Protection (**PDP Decree**), to which we have previously provided [comments](#)². It is our understanding that this Draft Decree will sit under the LOCS and seeks to consolidate the various administrative sanctions for violations under the Draft Decree on Cybersecurity (**Cybersecurity Decree**) and PDP Decree. We appreciate the Government of Viet Nam's continuous efforts to develop a legal framework for cyber and information security. We also acknowledge and recognize the important task that MPS has undertaken to ensure that Viet Nam is well-positioned to deter and manage different types of violations and threats in the cyberspace.

¹ The Global Data Alliance (globaldataalliance.org) is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. Alliance members are headquartered across the globe and are active in the advanced manufacturing, aerospace, automotive, consumer goods, electronics, financial services, health, media and entertainment, natural resources, supply chain, and telecommunications sectors, among others. BSA | The Software Alliance administers the Global Data Alliance. For more information on the Global Data Alliance, please see: <https://www.globaldataalliance.org/downloads/aboutgda.pdf>

² <https://www.globaldataalliance.org/downloads/en04092021gdavnppdp.pdf>

However, we are concerned that an excessively broad implementation of the LOCS and its corresponding draft decrees, especially in the context of cross-border data transfers, would be an ineffective method for achieving this goal and may have a chilling effect on innovation and investments. We offer the following comments in the hope that they will be helpful as MPS continues its efforts to finalize the Cybersecurity Decree and PDP Decree and consider their impact on the Draft Decree on Sanctions Against Administrative Violations in the field of Cybersecurity.

General Observations

At the outset, we would like to highlight that both the Cybersecurity and PDP Decrees are yet to be finalized even though the Draft Decree is meant to consolidate the various administrative sanctions for violations under the two aforementioned decrees. While we appreciate the level of transparency and stakeholder engagement demonstrated by MPS through this public consultation process, it is difficult for the industry to provide substantive input to the Draft Decree without a clear understanding of the obligations in the other two Decrees. In this regard, we urge the MPS to continue working with the industry on the draft Cybersecurity and PDP Decrees and to make the text of these two draft Decrees available to us for further comment and consultation.

Specific Comments and Recommendations

In this section, we provide comments and recommendations on Article 26 under Section 2, “Violations of Regulations on Personal Data Protection” and Article 37 under Section 4, “Violations of Regulations on the Implementation of Cybersecurity Protection Activities”.

Article 26 - Penalties Related to Cross-border Transfer of Personal Data

Article 26-1(a) states that a fine will be imposed if personal data of Vietnamese nationals were transferred without meeting all three conditions under paragraph 2 of Article 16 of the Decree on Personal Data Protection. Although the PDP Decree is not finalized and we do not know what the three conditions will be, we do note that Article 26-1(b) and (c) include references to “impact assessment” and legally binding agreements. In addition, there are also requirements in the Draft Decree for transferring organizations to notify the Personal Data Protection Authority of the transfer, and to retain dossiers of the impact assessment and/or legally binding agreements for audit purposes.

Taken collectively, we are deeply concerned with the restrictive requirements on cross border transfers of personal data. To require organizations to fulfill multiple conditions such as those described above before they are allowed to transfer personal data will undermine the ability of global companies to do business in Viet Nam and harm the ability of companies in Viet Nam to provide global services. The additional notification and retention obligations increases compliance costs on businesses while providing no practical value to data subjects and may inadvertently create new privacy and security concerns by forcing them to store and access data they otherwise would not. We urge MPS to revise the provisions in the draft PDP pertaining to cross-border transfer of personal data to allow for further flexibility.

Article 37 - Penalties Related to Data Localization

Article 37-2 specifies that a fine will be imposed if an organization fails to store data or establish a branch or representative office in Viet Nam as prescribed in paragraph 3 of Article 26 of the LOCS. Previous submissions on the Cybersecurity Decree have highlighted the need to clearly define the limits of the data localization and local office requirements.

Broad implementation of data localization and local office policies will negatively affect Viet Nam’s economic competitiveness as businesses across all sectors and of all sizes in Viet Nam rely on and benefit from the seamless flow of data into and out of the country. Data localization expenses will inevitably be passed along to consumers in the form of higher prices. Requiring local businesses to use

local data centers will add costs that are particularly hard to absorb for small and medium sized businesses. Ultimately, these localization requirements may also undermine cybersecurity by forcing companies to use potentially less secure local servers and to divert funds that could otherwise be focused on enhancing network security.

As Viet Nam continues to implement the LOCS, it should limit localization requirements only to the most sensitive national security data, if deemed necessary. This would enable specialized handling and localization of truly critical data and reduce confusion or uncertainty for international companies interested in investing or expanding investment in Viet Nam.

In addition, the scope for data localization requirements should also be narrowed to exclude organizations that do not disseminate information to the public, including, but not limited to, enterprise software and cloud service providers. We note that Article 26.1.c of draft Cybersecurity Decree (July 2019 version) requires businesses that have “*full knowledge of the fact that the service that the business in question provides is being used to commit acts of violation of Vietnamese laws...*” to store their data in Viet Nam. In the case of enterprise service providers, they typically do not have visibility or knowledge of the content their enterprise customers are uploading to their services, including whether that content constitutes data that would be in violation of Vietnamese laws. Hence, **we recommend that relevant obligations under the draft Cybersecurity Decree regarding data localization should not be applied to businesses that process data on behalf of enterprise customers.**

Conclusion

We would like to thank the MPS again for the opportunity to comment on the Draft Decree. We appreciate MPS's kind consideration of our above comments. For any questions or if any point of clarification is required on any part of this submission, please feel free to contact the undersigned at eunicel@bsa.org. Thank you for your time and consideration.

Sincerely yours,



Eunice Lim
Senior Manager, Policy
Global Data Alliance