CHAPTER 1 DIGITAL

OVERVIEW

Digital is a transverse tool for the economy, impacting all sectors and industries. Digital transformation accelerates and enhances traditional businesses and procedures, and this is paramount to remain competitive in this fast-changing economic world.

However, what exists in the real world still needs to be digitalised and a real change would be having legal electronic alternatives for wet signatures, personal identification, business licenses, and so on, without having to file a hard copy for compliance reasons. This would allow business or administrative procedures to be performed remotely.

Vietnam should aim to be an appropriate environment for companies to thrive by leveraging digital technologies. This is especially relevant in light of the global COVID-19 pandemic, where businesses and governments need to adopt new technologies and standards to compete in the global market.

The EVFTA is a milestone for Vietnam in its global integration. Yet, one of the biggest challenges at the moment is the COVID-19 crisis creating challenging conditions for trade. The Digital Sector Committee would like to suggest prioritising projects that will improve these conditions, involving international experts in dialogues to align with global standards.

Since the EVFTA entered into force on 1 August 2020, it has become the steppingstone to implement solutions that will enhance the digital economy. Vietnam is working on its Digital Transformation to reach its objectives by 2025-2030. To take advantage of the EVFTA and other trade agreements, Vietnam would need to facilitate cross-border trade more than it already does.

We believe that the following topics would be beneficial both at a national and global level:

- Cross-border electronic signature recognition to cover global agreements;
- Implementing platforms and tools towards traceability, the origin of goods, and transparency;
- Free movement of data across borders; and
- Adoption of internationally-recognised technology security standards.

E-government is a great step in this direction and the Digital Sector Committee is interested to see how it progresses. In this light, the topic of E-signatures becomes particularly important since it is the solution for businesses to continue operating when it has become difficult to sign in person.

We are keen to support the development of E-government and act as middlemen between Vietnam and the EU.

I. CYBERSECURITY

Relevant authorities: Ministry of Information and Communication (MIC), Ministry of Public Security (MPS); Office of the Government (OOG)

Issue description

It has become even more important to apply the Law on Cyber Information Security[1], which sets the cyber security standards and the Cyber Security Law[2], which frames the usage of digital services and ensures data sovereignty for national “data capital”. This regulation protects - in the broadest sense -

1 Law No. 86/2015/QH13 dated November 19, 2015 of the Government on Cyber Information Security.
2 Law No. 24/2018/QH14 dated June 12, 2018 of the Government on Cybersecurity law.

“subjects” on Vietnamese soil (for example, users using online services or accessing and transferring data) and establishes a framework and set of rules foreign companies in the Vietnamese market need to comply with. With these laws, Vietnam ensures its economic actors’ systems are adequately protected. It offers a reliable ground for business partnerships within and outside Vietnam to happen, as investors will trust the compatibility of the systems with international regulation.

Both EU and Vietnamese regulations compel companies to secure their systems at a technical level, preventing any leaks from a cyber-attack. However, there are still differences in the legal processing of the data and the privacy as mentioned below.

Following our analysis of the scope and application of the Vietnamese regulations, the following three challenges might exist:

- Making Vietnamese’s standards understandable for all stakeholders who must comply and bringing the same standards as written in the EU and its General Data Protection Regulation – (EU GDPR).[3]
- Addressing conflicts that may arise for companies already subject to the EU GDPR and for Vietnamese companies doing business with EU “data subjects” and that, therefore, need to comply with the EU GDPR.
- Finding a data policy that fulfils the Vietnamese Government agenda of data security while addressing the concerns of the business community. The economic impact of such policies needs to be considered.

1. Harmonisation of the Vietnamese regulation and GDPR

Ensuring efficient data transfer across borders underpins the digital economy and plays a fundamental role in driving the economy toward digitalisation. The establishment of a Facilitator to deal with conflicting cases in agreement with the Personal Data Protection Committee, or any relevant institution on the Vietnamese side, the European Data Protection Board and the European Commission, would assist in this regard. For instance, a facilitator could certify any Vietnamese company processing GDPR-protected data. Certification implies adherence to a code of conduct, where the said company states that it complies with the EU-GDPR standards to do business with EU partners.

The facilitator would handle any issues or difficulties between Vietnamese and European subjects. For example, any request relative to the Vietnamese Regulation that could conflict with the EU-GDPR would be addressed by the Facilitator.[4] Exceptional access to the EU-GDPR protected data can be granted under EU-GDPR Article 49 (Derogations) and in conformity with a Judiciary Agreement (EU-GDPR – Article 48) from the EU side. The Facilitator could be a newly-created institution consisting of a member of the Personal Data Protection Committee for the Vietnamese side and nominated members from the EU, or it could be included in a third-party institution, for instance at the ASEAN level.

As the EU-GDPR was adopted after the EVFTA was finalised, the EVFTA does not contain any relevant provisions. Therefore, a working group within the Trade Committee could be created to tackle this and other E-Commerce and digital issues. This working group could consist of experts under the European Commission or the platform under the EU-Vietnam Business Council. We also recommend

3 General Data Protection Regulation dated 14 April 2016 of the European Union.

4 For example, Article 21 CSL on the prevention and response to cybersecurity emergencies.

implementing the EVFTA by finding ways of consensus at two levels: first, through negotiation between the EU and Vietnam and, second through the practice of assessing cases.

We would suggest bringing the requirements under the EVFTA and the Vietnamese regulation in line with each other as this will ensure the stability of the national economy as well as facilitate bilateral trade. It is important to enable a public and transparent process, especially on such an important topic for the public related to the privacy of citizens.

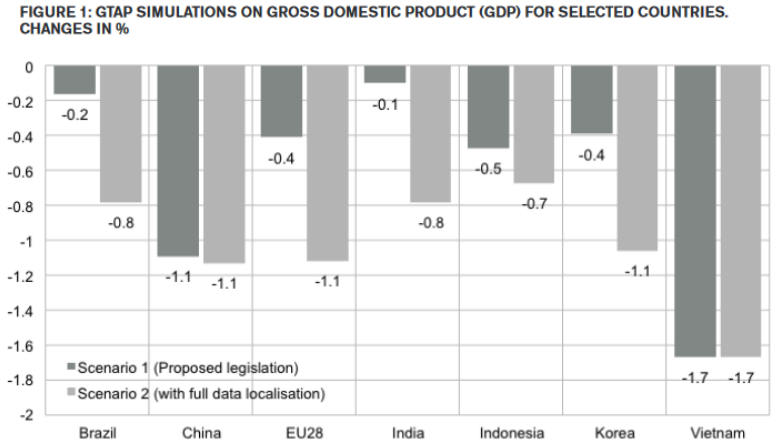
2. Impact on Vietnam's Economy

It will be disruptive and costly for Vietnamese companies that use global payment, social media, e-payments, smart technologies, cloud computing and advertising services to store data in Vietnam while the services from international providers are also not hosted in Vietnam. Businesses in Vietnam are leveraging ICT and other services to increase business and participate in cross-border trade.

Vietnam would become the only country in ASEAN with a broad national data residency law in the private sector.[5] To ensure Vietnam remains regionally competitive and aligns with best practices, the Government should adopt a data classification system whereby only public sector national security data must remain in Vietnam. China is often cited as a country with a successful data localisation policy, but this analysis fails to account for the differences in the economies of China and Vietnam. China has an enormous domestic middle-class market and local national champions that can provide all digital services locally. At its current stage of development, Vietnam relies on digital services that are provided by global companies to power its Fourth Industrial Revolution. As such, Vietnam would be better served by modelling its digital economy policies on countries with similar economic structures and at similar levels of development to Vietnam.

Vietnam stands to grow its GDP one per cent for every 20 per cent of spending on ICT, with mobile Internet accounting for 6.2 per cent of GDP and 3.2 per cent of total employment between 2015 and 2020. The government has targeted e-commerce spending to reach US$ 350 million annually, with B2C revenue rising to US$ 10 billion and accounting for five per cent of all retail spend.

Figure 5: GTAP simulations on gross domestic product (GDP) for selected countries



A previous study by the European Centre for International Political Economy found that Vietnam's data localisation policies will reduce Vietnam's GDP growth by 1.7 per cent.

5 Indonesia, which previously was a point of comparison, has allowed the majority of private sector data to be stored and processed offshore since October 2019.

3. Impact on Companies

Vietnamese companies compete on a global scale and, as a result, require cutting-edge resources and industry-leading security to ensure they remain competitive with their regional peers. The nature of forced localisation limits business' ability to access tools necessary to lower IT costs, innovate, and scale rapidly.

A report from the Leviathan Security Group shows that data localisation measures raise the cost of hosting data by 30-60 per cent. This is because the Internet enables centralised data storage and processing which results in economies of scale and a seamless, global internet resulting in lower costs.

Many Vietnamese enterprises and start-ups already use offshore ICT services to (1) improve security, (2) ensure quality control, and (3) access the most innovative services in data analytics, machine learning and "Internet of Things". If this will no longer be possible, companies will no longer be able to serve their customers efficiently. Companies which will be negatively impacted by such a requirement include:

- Vietnamese government owned and private airlines;
- National television networks;
- Subsidiaries in healthcare, ICT, car assembling, e-commerce of some large "national champions";
- Manufacturers of lighting and electrical equipment;
- Many start-ups with focus on payments to games, media and social applications;
- State-owned enterprises and Vietnamese private and public listed enterprises in finance, retail, real property, social media, are using global cloud-based accounting, productivity, and security services;
- Many banks and consumer financing companies, fully digitised or are digitising their processes and services; and
- Large government owned and private corporations and financial institutions using global banking services by international financial institutions.

The distinction between "domestic" and "foreign" enterprises would likely lead to significant confusion and disruption. For example, it is not clear if "domestic enterprises" would include Foreign Direct Invested (FDI) companies registered under the Vietnam Investment Law and incorporated in Vietnam (both wholly-foreign-owned and majority foreign-owned). If it does, these digital service providers in Vietnam will be required to store users' data in Vietnam. This is inconsistent with the business model of most multinational companies that provide digital services. Even if multinationals use some data storage services in Vietnam to reduce latency to customers, for many of these entities, most data processing and advanced analytics occurs offshore due to cost efficiencies and service improvement insights made possible through data aggregation. It is, therefore, unclear how multinationals providing digital services could continue operating in Vietnam if this data localisation requirement is implemented.

4. Impact on Security

The Government has the responsibility to ensure national security and protect its citizens. However, the data localisation provisions will not meaningfully improve security. Security is not related to the physical location of the data. The Internet is global, so any system connected to the Internet, directly or indirectly, is vulnerable to attacks (cross-border attacks and data breaches are the norm).

Security is fundamentally about (1) the security of the physical infrastructure where data is stored and (2) who owns and controls the data (and can, therefore, assist law enforcement). Vietnamese companies should be able to store and process their data in the most secure data centres, which independent third parties audit against global security and privacy standards. In this regard, only global service providers can provide this level of security.

EuroCham's Digital Sector Committee believes that it is possible to achieve the Government's underlying security/law enforcement access aims without imposing hard localisation requirements on domestic companies. In using international data services, domestic companies will continue to have effective control over their data regardless of where it is physically stored and can retrieve that data and/or provide access to that data to Vietnam law enforcement officials exercising their authority. This will not be limited by storing data offshore.

Potential Gains/Concerns for Vietnam

As set out before, the fact that the Vietnamese regulations possibly conflict with regulations from other regions might cause difficulties for businesses. For example, a Vietnamese business that collects and processes the personal data of data subjects in another country with strict data protection regulations (e.g. the EU GDPR) could be put in an untenable position with respect to how it processes the personal data of those data subjects. Compliance with the Vietnamese Regulation could be deemed incompatible with various EU requirements under EU GDPR.[6] In case both Vietnamese law and other laws govern a conflict, businesses would be confused about which regulation would be applicable and, therefore, might risk non-conformity with one regulation while adhering to the other, risking large fines. This might be a reason for a company to renounce developing its business in Vietnam. It is important to ensure compatibility between Vietnam and the EU with regards to Article 45 of the EU GDPR transfers based on an adequacy decision.

Recommendations

We would like to make the following recommendations[7]:

- Ensure compatibility between Vietnam and the EU with regards to Article 45 of the EU GDPR transfers on the basis of an adequacy decision including a concrete timeline and action list.
- Establish a Facilitator-institution to resolve conflicting cases with the agreement of the Personal Data Protection Committee, or any relevant institution on the Vietnamese side, the European Data Protection Board and the European Commission.
- Create a web portal which is accessible to foreign companies and includes practical guidance, training leaflets for staff, a forum, templates for the conformity files, basic consulting, and a list of consultants that could support with the implementation of the Vietnamese regulations' requirements.
- Start a process and create a working group to bring the EVFTA and the Vietnamese regulations in line with each other, addressing current conflicting situations.
- Classify the data processing and develop a data classification system whereby only national secrets must be onshore and other non-state secrets may be offshore to lower the economic impact on the local economy, especially more vulnerable start-ups, and small and medium sized companies.

6 For example, a Vietnamese data processor could have to share personal data in its system under the CSL article 21. If in the meanwhile this data is protected by the GDPR through Standard Contractual Clause, there is a conflict.
7 The Law on Cyber information Security (No. 86/2015/QH13) addresses the regulation of content related to cybersecurity for e-Government, for Cloud and Personal Data Security law so recommendations are given taken considering the provisions in that law.

- Remove the requirement on domestic enterprises to keep data in the country to enable cross-border data processing with data hosted offshore, to enable Vietnamese companies to have minimal costs on their IT systems and multinational companies to maintain their consistent global business models.
- Ensure there will not be conflicting provisions between the 2015 Law on Cyber Information Security and 2018 Cybersecurity Law and future decrees on personal data protection and cybersecurity being drafted.

II. E-GOVERNMENT

Relevant authorities: Office of Government (OOG), Ministry of Information and Communication (MIC)

Issue description

We applaud the Government's impressive progress in its Digital Government program in 2020. In the digital government journeys, the world's leading digital governments rely on the cloud's flexibility, innovation, and scale to empower officials with the insight they need to deliver top-tier public services. Modern governments work on the front lines of service delivery and face a challenging fiscal environment. With no room for administrative waste, governments increasingly need rapid access to technologies that simplify their processes, deliver massive reductions in administrative costs, and enable innovation to create efficient and effective citizen services.

In order to make further progress, it would be important to recognise certificates for electronic signatures issued to individuals. The foundation of a digitalised world is to provide electronic alternatives for wet signatures and personal identification. Aligning Vietnam's standards with those defined by The Electronic Identification and Trust Services Regulation (eIDAS)[8] would be the first step, expediting the regulation around the Electronic Signature standards and converging towards a global standard. Furthermore, governments issue policy statements with an actionable directive – including timetables – creating a framework for the implementation of cloud technologies, clarifying the roles and responsibilities of government entities and Cloud Service Providers (CSPs), and establish a procurement vehicle that is designed to gain the full benefits of cloud technologies. Governments use existing domestic and international cloud-centric accreditation systems to evaluate CSPs (rather than create their own unique certification programs) and leverage the shared responsibility model for cloud security. When government customers leverage third-party certifications, they avoid subjecting themselves to duplicating, burdensome processes or approval workflows that may not be required for a cloud environment. Using such accreditations also enables governments to build a more efficient and fast compliance process.

Governments categorise their data based on its level of sensitivity, and then manage each segment in a manner consistent with its level of sensitivity. Data classification helps organisations safeguard sensitive or critical data with appropriate levels of protection. Regardless of whether data is processed or stored in traditional on-premises systems or the cloud, data classification is a starting point for maintaining the confidentiality (and, potentially, the integrity and availability) of data based on the data's risk impact level. Reputable standards organisations, such as the International Standards Organisation (ISO) and the National Institute of Standards and Technology (NIST) of the United States Department of Commerce, recommend data classification schemes so that information can be more effectively managed and secured according to its relative risk and criticality, advising against

8 The Electronic Identification and Trust Services Regulation dated 23 July 2014 of the European Union.

practices that treat all data equally. Governments establish and/or adopt complementary security, data processing, and privacy policies to support a successful transition to cloud computing.

Governments retain full control and ownership over their data, and have the ability to choose the geographic location(s) in which it is stored. Cloud providers should also provide identity and access controls enabling government agencies to restrict access to their infrastructure and data. These are part of the important basic concepts regarding data ownership and management in the "cloud shared responsibility" model, and below are the four others:[9]

1. Governments can download or delete their data whenever they like.
2. Governments can "crypto-delete" their data by deleting the master encryption keys that are required to decrypt the data keys, which are, in turn, required to decrypt the data.
3. Governments should consider the sensitivity of their data and decide whether and how to encrypt the data while it is in transit and at rest.
4. Governments should ensure that CSPs provide documentation detailing how government agencies can use cloud services to meet specific compliance and data privacy/protection requirements, based on international standards.

Data residency requirements do not improve the overall security posture of an organisation. Governments should assess their data classification approach and hone in on which data needs to stay within their country or region, and why. By doing so, governments may find that their data, potentially even official or secret data, may be stored and/or replicated elsewhere if there is no particular legal or policy geographical requirement.

As technology continues to advance and change customer threat vulnerabilities and vectors, governments must re-evaluate how they are modelling their data management, privacy strategies, and risk tolerance. Three fundamental realities have disrupted the traditional 'full stack control' model of data management.

1. Most threats are exploited remotely. The physical location of data has almost no impact on threats propagated over the Internet.
2. Manual processes present risk of human error. Human process failure plays a role in root cause failure of most cybersecurity.
3. Insider threats prevail as a significant risk**.** The vast majority of data compromises occur either through unintentional error or intentional malicious behaviour through authorised accounts.

Breaches do not require physical access to a server, but instead exploit a lack of effectively implemented logical security controls. The best mechanism to protect, detect, respond, and recover is to use the transformational security a CSP offers through modernisation and automation.

Potential Gains/Concerns for Vietnam

In recent years, governments around the world have started adopting policies that encourage government agencies to use cloud computing services. The reason for this is that governments recognise the role cloud computing can play in creating better citizen services and facilitating collaboration and data sharing between government agencies. Infrastructure transformations can

9 Some references can be found here: European Regulation on Data Protection: https://gdpr.eu/, European Mechanism of Standard Contractual Clauses : https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, Singaporean Regulation on Data Protection: https://sso.agc.gov.sg/Act/PDPA2012, Singaporean Model Contractual Clause: https://www.aeilegal.com/tldr/asean%20data%20mgmt, UK Government Security Classifications: Government-Security-Classifications-Supplier-Briefing-Oct-2013.pdf (publishing.service.gov.uk), US National Security Classifications: The President Executive Order 13526 | National Archives, Phillippines' Cloud First Policy: DICT Releases Amended Cloud First Policy for Gov't Transition to "New Normal" | DICT.

benefit governments and their citizens by galvanising innovation, facilitating inter-agency collaboration, and accelerating the timetable for services to reach constituents. We are pleased that Vietnam has issued Decision No. 942/QD-TTg approving the Strategy for E-Government Development towards Digital Government in the 2021-2025 period, with a vision to 2030 which sets out the vision for Central Government Cloud, Agency Government Cloud and Enterprise Government Cloud.

Recommendations

We would like to make the following recommendations:

> Develop and adopt smart cloud policies to accelerate digital transformation implementing the best practices identified and set out in the beginning of this paragraph allowing a transition to a secured, digitalised environment related to:
  - Recognition of certificates for electronic signatures issued to individuals
  - Promoting cloud-first policies
  - Cloud accreditation, compliance, and security
  - Data classification
  - Data privacy and control
  - Data residency
  - Perform a risk and threats assessment (remote access, manual processes presenting a risk of human error and insider threats)

ACKNOWLEDGEMENTS

EuroCham Digital Sector Committee.