Rödl & Partner

CLIENT ALERT VIETNAM

Issue:
October
2018

MANAGING CHANGE

Latest News on cybersecurity law in Vietnam

www.roedl.de/vietnam | www.roedl.com/vietnam

Rödl & Partner

CLIENT ALERT VIETNAM

Issue:
October
2018

MANAGING CHANGE

Read in the issue:

→ Law on cybersecurity

→ Law on cybersecurity

On 12 June 2018, National Assembly of Vietnam has adopted the Cybersecurity Law (CSL) regulating activities on protection of national security and social orders on Vietnam cyberspace.

CSL shall come into its effectiveness on 1 January 2019. Upon its effectiveness, enterprises providing services on Vietnam cyberspace must fulfil various cybersecurity obligations. Due to the broad of its governing scope, CSL could potentially impact any company with operations or services available for use in Vietnam, from a business, data collection data processing and storage perspective.

Overview

CSL requires the establishment of a comprehensive graded protection regime for cybersecurity, including various general obligations and a number of requirements which specifically apply to the followings:

- Enterprises providing services on the telecom network, internet and value added services on cyberspace in Vietnam (ISPs);
- Information system administrators (ISAs);
- Cybersecurity Authority (CA); and
- Individuals, organizations being active on the cyberspace.

All provisions under the CSL are aimed to protect and enhance the cyber sovereignty, cybersecurity of Vietnam. As such, CSL is structured in a way that all of the illegal acts as below shall be handled and eliminated:

- Using cyberspace, information technology and electronic media in order to breach the law on national security, social order and safety.
- Cyberattack, cyberterrorism, cyberspionage or cybercrime
- Obstructing or disrupting the operation of the cyberspace in Vietnam.
- Opposing or obstructing the activities of CA.
- Illegally attacking, neutralizing, disabling or rendering ineffective any cybersecurity protective measures.
- Abusing or misusing cybersecurity protective activities in order to violate national sovereignty, interests or security, social order or the lawful rights and interests of agencies, organizations and individuals, or for personal profit.

Key issue

CYBERSECURITY OBLIGATIONS OF ISPS

CSL requires the establishment of a comprehensive graded protection regime for cybersecurity including obligations for ISPs as below:

- Filtering: ISPs must filter published information upon requests of in charge State-authority in case of occurring cyberattack that infringes or threatens to infringe national sovereignty, interests and security and/or causes serious harm to social order and safety to ensure that contents of those information to eliminate the cyberattack as well as to provide all related information on a timely manner.
- Personal data verification: ISPs must set up adequate mechanisms to authenticate information when users register digital accounts;

- Information interference upon request: ISPs must prevent the sharing, deleting of information containing any illegal content propaganda against the Socialist Republic of Vietnam, instigate violent disturbances, disrupt security or disturb public order, are embarrassing or slanderous, or are in violation of the economic management order ("Information Against the State") directly managed by Cyberspace Service Providers within 24 (20) hours from the time requested by the CTF under the Ministry of Public Security or competent authorities under the Ministry of Information and Communications.
- Suspension or termination of provided services upon request: ISPs must promptly suspend the production of digital devices and the provision of cyber services and applications, and give timely notifications to related parties and to take remedial actions when any of their digital devices, cyber services, or applications has been discovered to have possibly disrupted cyber security.
- Warning of the possibility of a loss of cybersecurity: to give warnings of the possibility of a loss of cybersecurity during the use of the services in cyberspace provided by such enterprise and to provide guidelines on preventive measures.
- Handling of cybersecurity incidents: to formulate plans and solutions to quickly respond to cybersecurity incidents, and to immediately deal with any security weaknesses or vulnerabilities, malicious codes, cyberattacks, cyber intrusions/infringements or other security risks; and when a cybersecurity incident occurs, to immediately implement appropriate emergency plans and response measures, and at the same time provide a report thereon to the State-authority in charge.
- Data protection: to implement technical measures and other necessary measures to ensure security during the process of collecting information and to prevent the risk of revelation, damage to or loss of data; and in the case of occurrence or possible occurrence of the revelation, damage to or loss of data about user information, to immediately provide responsive solutions, and at the same time notify the user and report to the State-authority in charge.
- Coordinating with the State-authority in charge: coordinating and facilitate State-authority in charge to conduct their cyber-security protective activities.
- Notification: timely notifying State-authority in charge for any signals of cyberterrorism.

Moreover, if ISPs engage in the activities of collecting, utilizing, analyzing and processing personal data, data relating to the relationship of the users, data generated by the users in Vietnam ("ISPs 1"), such ISPs 1 shall have following obligations in addition to the aforementioned ones:

- Establishment of commercial presence: ISPs 1 must set up its commercial presence in Vietnam either under the form of a representative office or a branch; and
- Filing system: ISPs 1 must store users' data generated in Vietnam within a statutory period of time. CSL however does not clarify if the data/information to be stored in Vietnam would only be the data of Vietnamese citizens residing in Vietnam. It is thus questioned whether or not data of EU citizens living in Vietnam or data of Vietnamese living overseas must be stored as well. Furthermore, it is unclear whether the requirement on storing such data in Vietnam shall mean such data:

  (i) must be stored exclusively in Vietnam; or
  (ii) ISPs 1 must set up its server in Vietnam to store the data.

CYBERSECURITY OBLIGATIONS OF ISAS

ISAs, as defined under the Decree 85/2016/ND-CP on the security of information system by classification, are "authorities, organizations and individuals given authority to manage the information system directly. In government bodies and agencies, administrators of information systems refer to ministers, ministerial-level bodies, government agencies, provincial People's Committees or entities given discretion in investment projects for the construction, configuration, upgrade and expansion of such information systems." CSL stipulates that ISAs must comply with a series of requirements designed to prevent and handle violations of cybersecurity. These requirements consist of:

- Implementing necessary managerial and technical measures: to prevent, detect, block and/or remove (i) Information Against the State and cyberattacks upon requests of the State-authority in charge; and (ii) any acts of cyberespionage, infringements of State secrets, work secrets, business secrets, personal secrets, family secrets or private life on the information system and to promptly remove any information related to such conduct.
- Inspecting cybersecurity: to detect and remove malicious codes and malicious hardware and to remedy security weakness and vulnerabilities; and to detect and deal with unlawful infringement activities or other threats to cybersecurity.
- Coordinating with and implementing requests of the CA: to prevent and combat cyberespionage, and in order to protect information classified as State secret, work secrets, business secrets, personal secrets, family secrets or private life on the information system.
- Collecting evidence of the cyberattack: applying measures as requested by the CA to determine the origin of the cyberattack and collect evidence of the cyberattack.
- Reviewing information system: regularly reviewing and inspecting information system to eliminate cyberterrorism threats.
- Notification: notifying the In-charge Division of the Ministry of Public Security upon discovery of any breach of the law on cybersecurity on the information system within its scope of management.

OBLIGATIONS OF INDIVIDUALS AND ORGANIZATIONS

Individuals and Organizations being active on the cyberspace must comply with all cybersecurity regulations. Amongst the many stipulated obligations, critical obligations are implementing requirements and guidelines of competent agencies during cybersecurity protection.

CYBERSECURITY AUTHORITY

4 State-authority bodies mainly in charge of controlling and managing cybersecurity under the CSL are:

- Ministry of National Defence.
- Ministry of Public Security.
- Ministry of Foreign Affairs.
- Ministry of Information and Communications.

Each of the above Ministry shall have their own division focusing on addressing cybersecurity issues, in which such special divisions of Ministry of National Defence and Ministry of Public Security are called Cybersecurity Task Force (CTF).

POWER OF CA

CA is empowered to carry out certain acts to protect cybersecurity. Main authority of Cybersecurity Authority are:

- Evaluation of cybersecurity: CA shall review and assess cybersecurity contents in order to provide the basis for a decision on constructing or upgrading an information system.
- Assessment of cybersecurity conditions: CA shall review whether an information system satisfies cybersecurity conditions prior to its being commissioned for operation and use.
- Auditing cybersecurity: CA shall identify actual cybersecurity status of the information system and of its infrastructure or of information stored, processed and transmitted on it, aimed at preventing, detecting and dealing with any cybersecurity threat and proposing plans and measures to ensure normal operation of such system.
- Suspending the provision of network information: CA is authorized to prevent, request for the suspension of provision of network information. In addition, CA is also entitled to suspend or temporarily suspend acts being the establishment, supply and use of telecom networks, of the Internet or being the manufacture and use of radio transmitters and receivers.
- Removing information: CA is authorized to demand the removal, access to unlawful or false information in the cyberspace infringing national security, social order and safety, or the lawful rights and interests of agencies, organizations and individuals.
- Collecting data: CA is empowered to collect e-data related to acts in cyberspace infringing national security, social order and safety or the lawful rights and interests of agencies, organizations and individuals.
- Restricting the operation of information system: CA can suspend or require the

cessation of operation of information systems or withdrawing domain names.

LEGAL CONSEQUENCES

Failure to comply with provisions under the CSL shall result in:

- Administrative liability, i.e., monetary penalty, remedial actions;
- Criminal liability;

Conclusion

- The CSL establishes a comprehensive legal framework in Vietnam for cyber sovereignty and cybersecurity. It is sweeping in scope, potentially affecting every company involved in the cyberspace, whether under Vietnam or foreign ownership, as even the activities of operating a website, offline network or company intranet would all fall within its scope. Prior to its effectiveness on 1 January 2019, companies with operations or services available in Vietnam should begin to assess the potential impact of the CSL both in terms of its business generally and its network infrastructure particularly. An ISPs having the activities of collecting customer information will be likely to be substantially impacted.
- Certain ISPs using encryption technology to handle data of its users are likely to encounter obstacles in complying with all obligations for ISPs, for example, filtering requirement.
- ISPs, ISAs having its operation activities around the globe should also assess the application of CSL in light of General Data Protection Regulations of the European Parliament and of the Council ("GDPR"). Whilst it is the obligations of ISPs and ISAs to hand over the CA requested data, the transfer of personal data of EU citizens generated in Vietnam or Vietnamese living in the EU to Vietnamese authority could result as a serious breach of the GDPR.

Contact for more information

Stefan Ewers, LL.M. (Melbourne)
Partner
Attorney at Law (Germany)
Registered Foreign Lawyer (Vietnam)
Head of Ho Chi Minh City Office
T +84 2873 072 788
stefan.ewers@roedl.com

Imprint

Publisher:
Rödl & Partner
20/F, CJ Tower,
2bis-4-6 Le Thanh Ton,
Ben Nghe Ward, Dist. 1,
Ho Chi Minh City, Vietnam
T +84 2873 072 788
www.roedl.de
www.roedl.com

Responsible for the content:
Rödl & Partner (Vietnam)
hochiminhstadt@roedl.com
20/F, CJ Tower,
2bis-4-6 Le Thanh Ton,
Ben Nghe Ward, Dist. 1,
Ho Chi Minh City, Vietnam

Layout/Type:
Rödl & Partner (Vietnam)
hochiminhstadt@roedl.com