IPS Institute for Policy Studies and Media Development

UNDP

REPORT

Review of Local Governments' Implementation of

PERSONAL DATA PROTECTION

on Government-Citizen Interaction Interfaces

Review of Local Governments' Implementation of Personal Data Protection on Government-Citizen Interaction Interfaces, 2022

The 2013 Constitution and other laws recognize privacy as a fundamental right in Viet Nam. As digital transformation of the public sector accelerates, a large amount of data on personal information is collected via tools, such as electronic provincial government portals (e-government portals), online public administrative services (e-service portals), and smart applications put into use by People's Committees at the provincial level. However, protecting personal data and ensuring user privacy on those platforms have not received adequate attention. There are still several gaps in the policies of those platforms to meet the current legal provisions, especially in comparison with good practices.

Within this context, based on the current legal framework, this study evaluates the personal data and privacy protection practices on e-government portals and online public service portals of all 63 provinces and municipalities as well as smart applications being put into use by 50 provinces. It aims to provide policy and practical recommendations for central and local government agencies on how to improve personal data and privacy protection on online government-citizen interaction interfaces at the provincial level in Viet Nam. Two dimensions were assessed: (i) privacy policies issued by local governments (whether privacy policies specify government agencies responsible for protecting privacy; types of information collected by local governments; with which third-party agencies the personal information is shared; children's privacy regulations, etc.); and, (ii) specific measures to implement such policies through technical tools. At the same time, based on the United Nations' principles on personal data protection, this study evaluates the personal data protection practices of local governments according to six criteria: (i) fair and legitimate processing; (ii) purpose specification; (iii)proportionality and necessity; (iv) retention principle; (v) transparency; and (vi) accountability in the collection and processing of personal data.

Status of personal data and privacy protection on online government-citizen platforms at the provincial level

Some localities have been building and deploying different tools to protect personal data and privacy on interactive platforms. However, in general, the authorities of the provinces and municipalities have not paid adequate attention to this aspect. None of 63 provinces have set a good practice in all respects but some have accomplished in some indicators. Only 4 out of 63 e-government portals and 3 out of 63 e-service portals have published a document on personal data and privacy protection (commonly referred to as the Regulations). Of the 50 provinces that operate smart apps to interact with citizens, 32 have posted privacy protection policies as required by Google Play and Apple Store.

The policies and tools related to personal data and privacy protection on e-government portals, e-service portals, and smart applications of provinces and cities deem spontaneous and do not stem from explicit awareness of the importance of privacy. Localities pay more attention to technical requirements to ensure the safety and security of data, prevention of cyber risks, and cyber security rather than personal data privacy and users' privacy. Although the documents issued by the local government on information security can be easily accessed online, of all 63 provinces, there are no documents on personal data protection on 59 e-government portals and 60 e-service portals. Moreover, most provincial platforms only require users to confirm that the information they provide is accurate but do not have tools for users to express their privacy preferences.

In addition, none of the above-mentioned policies and platforms fully meet the requirements of the law related to privacy in the digital environment based on 17 sub-criteria evaluated in this report, as well as 6 principles of the UN on the protection of personal data and privacy. Specifically, out of 39 privacy policies reviewed, 16 are publicly available only in English rather than in Vietnamese, and 22 are in Vietnamese rather than both. These sets of privacy policies do not regulate protection of children's information and privacy but do collect information beyond the allowed limit. They do not refer to a legal basis, specify the purpose of collecting personal information, or indicate people's right to give consent to or to disagree with the governments' collection of personal information. There is also a lack of tools for users to express their right to access information, request for the correction of information, file a complaint, etc.

In particular, except for the smart application of Hau Giang province, privacy policy documents on other provinces' smart portals and applications do not clearly define the legal relationship between the government agencies accountable for personal data collection and processing. Due to the lack of clarity on who is in charge of data control and management, the legal accountability for personal data collection and processing is confused between the "governing body" (Provincial People's Committees), the "operating agency/unit" (Departments of Information and Communications), and platform developers (service providers). Only 1 out of the 39 reviewed privacy policies states that the Provincial People's Committee is accountable for personal data collection, processing, and detention on the e-portals and smart applications. At the same time, the Department of Information and Communications is the agency operating and processing data on these platforms on behalf of the Provincial People's Committee. This situation is concerning as it is creating a gap of responsibility for personal data and information collected via government platforms. Moreover, it provides vague grounds for determining the responsible subjects and the responsibility of storing, managing, using, and sharing huge volumes of data after being collected from users through the local governments' interactive platforms.

Overall, considering the privacy protection in the entire process of local government interaction with citizens in the digital environment, it can be said that the input factors such as facilities and infrastructure have been provided with much attention. However, the implementation of personal data and privacy protection policies and laws requires further improvements. In particular, the outputs, including the degree to which personal data is protected, have not met the provisions of the 2013 Constitution, the Law No. 86/ 2015/QH13 on Cyber Information Security, the Law No. 67/2006/QH11 on Information Technology, the Decree No. 47/2020/ND-CP on management, connection and sharing of digital data of State agencies, the Decree No. 64/2007/ND-CP on information technology application in activities of State agencies, the Decree No. 43/2011/ND-CP stipulating the provision of information and online public services on websites or portals electronic government agency, and the Circular No. 25/2010/TT-BTTTT regulating the collection, use, sharing of personal information and measures to ensure safety and protect personal information on websites or electronic portals of State agencies.

Recommendations

Enhancing the national regulatory framework on personal data and privacy protection

At the national level, relevant legal documents need to regulate the following issues related to the protection of personal data privacy:

Firstly, it is required to explicitly define and classify personal data in line with the latest digital transformation trends, including types of personal data collected from users on interactive government platforms. At the same time, it is vital to distinguish between data privacy and data

security as privacy is concerned with protecting people's privacy, while data safety and security focus on protecting the information system and security of State agencies with technical tools.

Secondly, it is necessary to distinguish between data controllers and data processors, thereby explicitly defining the legal responsibilities of those subjects towards personal data subjects**.** The regulatory frameworks shall establish the default liability of the State agency when publishing the privacy policy document; or when they provide tools for people to express their rights, such as the right to agree or disagree with the provision of personal information on smart applications. Similarly, it is necessary to clarify the legal relationship between a State agency that collects personal data and an enterprise providing an interactive platform in the digital environment.

Thirdly, the responsibilities of relevant agencies should be clearly defined, and the processes and procedures for transparency in using and sharing personal data within State agencies and with external entities should be standardized. This is of importance in the context of a massive volume of personal data collected through government interaction platforms with citizens, with great concern about how to ensure data protection and privacy during storage, use, and subsequent sharing.

Fourthly**,** relevant laws should contain provisions on assigning personnel in charge of personal data protection and privacy in State agencies' activities, at least at the provincial level. The profile and contacts of this person should be published for citizens to liaise with when needed. This person is responsible for providing advice to local government agencies on personal data protection and privacy; monitoring local governments' compliance with legal regulations, common standards, and internal rules on privacy and personal data protection; and serving as a contact point between personal data providers and data governing bodies when necessary.

Fifthly, to achieve consistency across all provinces in personal data and privacy protection practices, it is important to regularly evaluate and research best practices, thereby forming specific regulations and guidelines for localities to grasp and gradually adopt the standards and providing a legal basis for efficient privacy protection in the digital environment. The Ministry of Information and Communications shall develop sample privacy documents for local government agencies to apply when providing online public services to ensure standardized personal data and privacy protection. These shall include, inter alia, sample privacy policy and sample terms of use between the responsible government agencies and users, and a sample contract between the government agencies and service providers of interactive government-to-citizen platforms.

Improving personal data and privacy protection in the local digital environment

Good privacy practices at the provincial level from this study show three important actions for local governments to consider: developing localized rules, focusing on the implementation process, and meeting the rights and interests of citizens. Personal data and privacy protection policies, as well as practical tools to implement those policies on interactive government platforms, need to closely follow and meet all requirements under 17 contents provided in relevant Viet Nam's laws and regulations that this report has covered. In particular, there should be clear identification of the main responsible agency, tools, and channels to receive comments or complaints about personal data and privacy violations, and public feedback on the quality and effectiveness of privacy protection.

This study emphasizes the importance of meeting the rights and interests of citizens who use services, products, and tools on e-government portals, e-service portals, and government smart applications. The level of local governments' performance in this aspect can be assessed based on the UN criteria on personal data protection and privacy. Accordingly, local governments can identify performance aspects that need to be adjusted and improved so that personal data and privacy are better protected. Specifically, local authorities can develop specific measures and tools to ensure the legitimacy and

lawfulness of processing personal information; collecting and using personal information for specific purposes; collecting personal information limited to the stated purpose, based on necessity; specifying durations of information storage; and increasing transparency and accountability in the collection, processing, storage and use of personal information.

Recommendations for evaluating personal data and privacy protection performance by State agencies on electronic and digital platforms

The report recommends that the review of government performance in the protection of personal data and privacy be expanded to all levels of governments, not only local governments. The report suggests that indicators and targets on personal data and privacy protection be added to the national digital transformation goals so that the digitalization efforts aim at not only improving quantity but also quality, as well as achieving the ultimate goal of ensuring the legitimate rights and interests of the people.

At the same time, the government should invest more resources in conducting an in-depth review of personal data protection and privacy practices by State agencies at all levels. The review should not only be limited to e-government portals, service portals, and smart applications, but also to databases managed by State agencies, where personal data is stored, used, and shared after being collected from interactive platforms.