: Level 18 - 789 Office Tower,
No. 147 Hoang Quoc Viet,
Cau Giay, Hanoi, Vietnam
: +84 941 236 233
: vtn-partners.com

BONES OF CONTENTION UNDER THE DRAFT LAW ON PERSONAL DATA PROTECTION

CONTACT US

For further information or assistance, please contact the following VTN professionals:

NGUYEN HUNG HA

Managing Partner

+84 365 888 396

ha.nh@vtn-partners.com

NGUYEN THANH NGHIEP

Partner

+84 982 450 996

nghiep.nguyen@vtn-partners.com

The Ministry of Public Security of Vietnam (MPS) has recently issued the draft of the Personal Data Protection Law to regulate matters pertaining to the safeguarding of personal data. In general, this draft offers a comprehensive legal framework and guidelines regarding the data protection matter in Vietnam and MPS's endeavors to contribute to data safety.

However, it presents several ambiguities that require careful scrutiny and amendment in future versions. While many provisions remain consistent with Decree 13, such as the 11 rights of data subjects, privacy notices, and consent requirements, there are multiple areas that demand further clarification:

Lack of Provisions for Processing Data for Legitimate Interests

There is an absence of an explicit provision allowing the processing of personal data for the legitimate interests of data controllers and processors. This is a significant gap, as legitimate interest is often a lawful basis for data processing in many jurisdictions, providing flexibility for various commercial activities. This point has been raised by loads of advocates through the first date of Decree 13.

Ambiguity Regarding Consent from Children and Guardians

The draft remains unclear regarding the precedence of consent between children and their guardians. Questions arise as to which consent should prevail in cases where both a child and their guardian are involved, especially under complex family dynamics or where children may have opposite views on their rights and interests.

Disclaimer:

The article cannot and does not contain any legal advice. The information is provided for general informational purposes only and is not a substitute for professional advice.

Accordingly, before taking any actions based upon such information, I encourage you to consult with the appropriate professionals. The use or reliance of any information contained in this article is solely at your own risk.

Insufficient Clarity on Marketing and Advertising Data Protection

The clause concerning personal data protection in marketing and advertising has been bifurcated into two separate rules, however, the distinction between these rules lacks sufficient clarity. It appears the separation is based on the medium of Internet usage, but the definitions remain vague, thereby risking inconsistent interpretations and compliance challenges.

Besides, the marketing service providers are prohibited to outsource any parts of their services.

Vague Regulations for Emerging Technologies

Rules governing personal data protection in big data processing, artificial intelligence, and cloud computing are introduced, yet the draft provides only vague stipulations on licensing requirements for processors in these domains. Moreover, the requirement for cloud service users to include specific contractual provisions with service providers seems impractical, potentially imposing undue burdens that many users may find impossible to meet.

Conflict with Employers' Rights in Employment Data Processing

There is a conflict between the data processing rules set forth in the draft and the legitimate interests of employers. Employers have a legitimate need to verify the qualifications of their candidates and employees, however, the current draft appears to limit such practices, thereby hampering the ability to maintain adequate workforce standards. Especially, after a recent judgment in terms of the unilateral termination of the employee by a local court in the north of Vietnam, the concern over employees' personal data protection is controversial.

The intra-group companies must enter into proper data processing agreements on the sharing of personal data overseas.

Heightened Requirements for Financial Sectors

The draft law imposes heightened personal data protection requirements on sectors such as insurance, banking, and financial services. Specifically, credit scoring, credit information services, data masking, and the transfer of personal data in reinsurance are subject to stricter standards, which may add complexity for these industries in ensuring compliance.

Additionally, this draft legislation introduces several regulatory and operational challenges regarding the complexities around regulatory oversight, certification requirements, and the absence of exceptions for impact assessments. These challenges can be enumerated as follows:

Citizen Credit Scoring and Regulatory Oversight

The draft establishes the concept of competent authorities overseeing citizen credit scoring in accordance with human rights as stated under the Constitution.

Certification and Expertise Requirements

Personal data protection service providers must meet stringent regulatory conditions, including employing certified experts in technology and law with appropriate credentials and maintaining a personal data protection credit rating of at least "Pass." Furthermore, they are required to obtain approval from a delegated agency under the Ministry of Public Security, which could impose additional administrative burdens.

Certified experts involved in personal data protection services are required to hold suitable academic degrees and complete mandatory training courses. While certification is mandatory for ensuring data protection standards, these requirements must be clearly defined to avoid obscurity in implementation.

Unclear Scope of Personal Data Protection Services

The draft remains vague concerning the scope of services that personal data protection providers are authorized to perform, including data protection officer services, personal data protection ratings, and personal data processing services. The lack of elaboration leaves service providers uncertain about their roles and responsibilities.

No Exceptions for Impact Assessments

The absence of carveouts or exceptions for data protection impact assessments (DPIAs) and overseas data transfer impact assessments raises concerns about the administrative load. This could mean that even routine activities, such as sending an email containing personal data overseas, may require extensive assessments, thereby creating onerous compliance obligations for organizations. The DPIA dossiers also require a document demonstrating the organizations' personal data protection ratings that put an additional burden on the whole system.

In conclusion, the detailed ambiguities and overarching challenges present in the draft highlight the urgent need for refinement and practical adjustments to facilitate effective implementation. Addressing these issues is essential to ensure that the legislation provides clear guidance for stakeholders.

Periodic Impact Assessment Updates

The draft mandates regular updates to impact assessment dossiers for any changes, excluding certain extraordinary circumstances like dissolution, mergers, changes in data protection officers, service providers, or business lines. This provision implies a continuous obligation to monitor and update, which may be burdensome for companies undergoing frequent operational changes.

Inconclusive Safeguards

The draft does not specify updates to personal data protection safeguards—whether technical or organizational. This omission may result in a lack of clear guidance on how organizations should evolve their data protection strategies in response to emerging threats and technologies, leading to potential vulnerabilities.