HOW SMALL BUSINESSES STRUGGLE WITH DATA PRIVACY – AND HOW THE NEW DATA LAW COULD CHANGE THE GAME

LEGAL INSIGHTS

MARCH 2025

QUOC & ASSOCIATES

INTRODUCTION

In Vietnam's rapidly evolving digital economy, data security is a crucial concern; however, many small and medium-sized enterprises (SMEs) struggle to comply with data protection regulations due to limited resources and expertise. The 2024 Annual Report by the Authority of Information Security (AIS) under the Ministry of Information and Communications (MIC) reveals that over 70% of SMEs lack comprehensive data protection measures, exposing them to cyber threats and regulatory risks. With the introduction of Decree No. 13/2023/ND-CP on Personal Data Protection and Law No. 60/2024/QH15 on Data, the Vietnamese government intends to enhance data security compliance. This article explores the key challenges SMEs face in managing data and how the new legal framework is poised to reshape the regulatory landscape.

I. CHALLENGES FACED BY SMALL BUSINESSES IN DATA SECURITY

II. HOW THE NEW DATA LAWS COULD CHANGE THE GAME FOR SMALL BUSINESSES

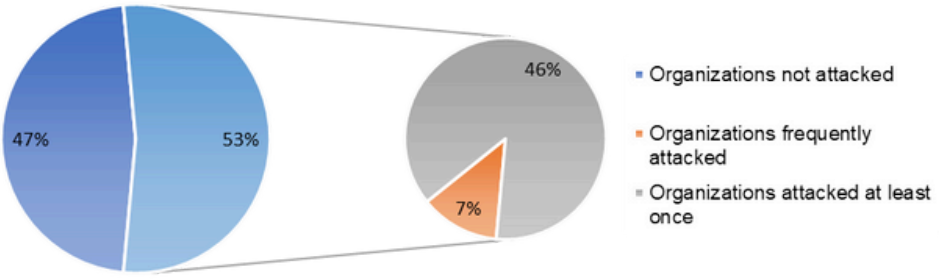
III. WHAT SMEs NEED TO DO TO COMPLY WITH DATA PROTECTION LAWS AND ENSURE BUSINESS OPERATIONS?

1 CHALLENGES FACED BY SMALL BUSINESSES IN DATA SECURITY

SMEs in Vietnam often lack the resources to fulfill data security requirements. Below are some key challenges identified in official reports:

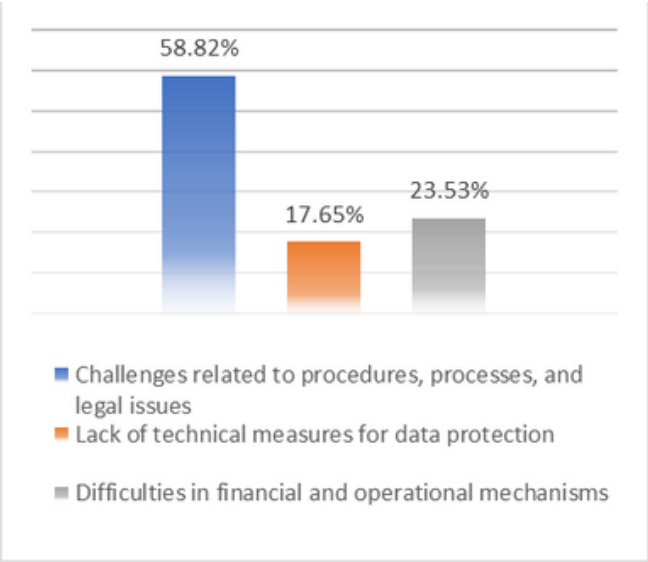
1. Lack of Understanding of Data Protection Laws

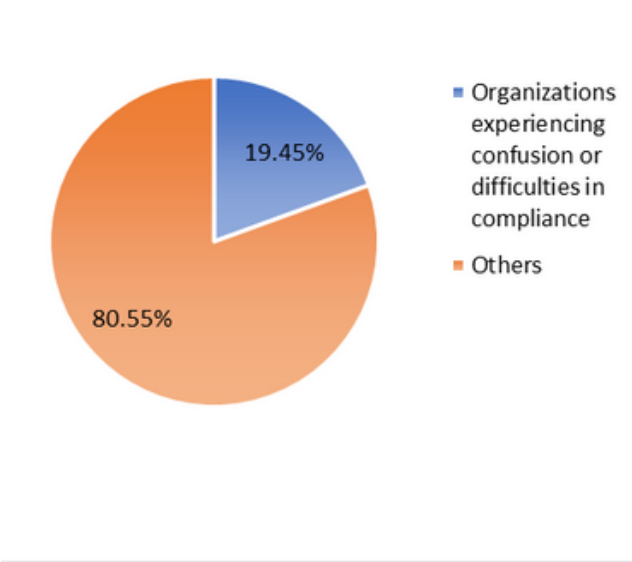
The 2024 Cybersecurity Summary Report for agencies and enterprises reveals that 46.15% of organizations experienced at least one cyberattack in the past year, with 6.77% facing frequent attacks. The total number of cyber incidents in 2024 is projected to exceed 659,000, and 14.59% of organizations reported ransomware attacks, resulting in significant financial and reputational damage.



Despite these threats, only 56.53% of organizations have dedicated personnel for personal data protection, while 43.47% either lack specialized staff or depend on part-time personnel. Furthermore, 19.45% of agencies and businesses struggle with compliance due to legal and procedural complexities.

A substantial number also lack the technical expertise necessary to implement basic security measures, such as encryption and secure data storage. Among the issues raised, the survey revealed that the most significant challenge lies in legal, procedural, and regulatory complexities, accounting for 58.82%, followed by the absence of technical measures for data protection at 17.65%. The survey identifies regulatory complexity as the primary challenge, highlighting the need for clearer legal guidance and stronger cybersecurity measures.





I. CHALLENGES FACED BY SMALL BUSINESSES IN DATA SECURITY

2. Financial Constraints.

Complying with personal data protection regulations requires significant investment in cybersecurity infrastructure, including security software, hardware, and secure storage solutions. However, SMEs often struggle to allocate resources for these investments. At the Government Standing Committee Conference on February 27, 2025, where breakthrough strategies for SMEs were discussed, only 30% –35% of SMEs reported access to preferential loans for cybersecurity investments. This highlights financial constraints as a major barrier to regulatory compliance. Additionally, businesses are expected to allocate at least 10% of their budget to cybersecurity, IT, and operational activities – an obligation many SMEs cannot meet. Compliance costs extend beyond infrastructure to include security tools, employee training, and legal consultations, placing further strain on limited financial resources.

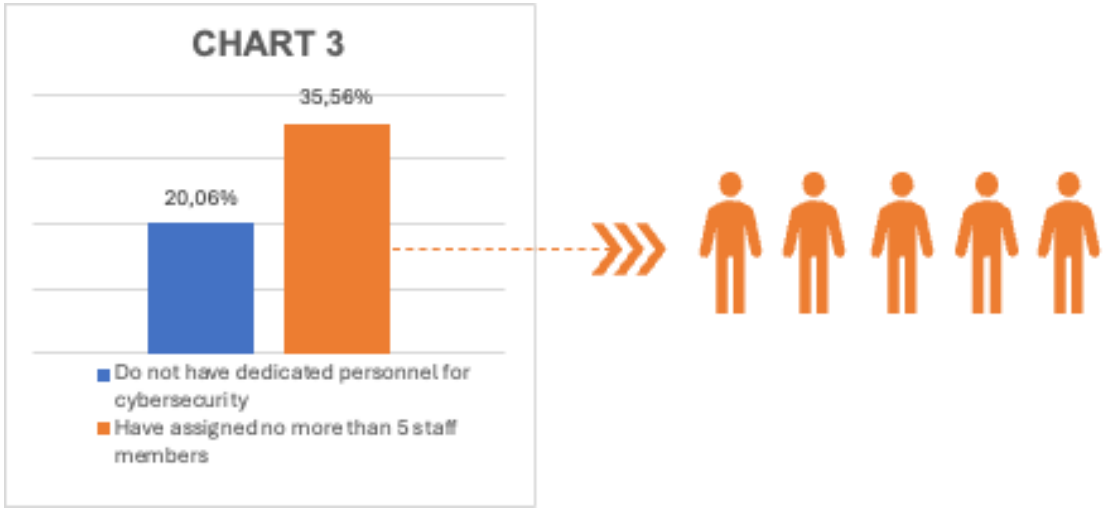
Despite government support programs, access remains limited. Only 25% of SMEs have benefited from credit packages supporting digital transformation and data security. This underscores the financial challenges SMEs face in meeting data protection requirements, often forcing them to absorb costs independently without adequate external support.

I. CHALLENGES FACED BY SMALL BUSINESSES IN DATA SECURITY

3. Lack of Structured Data Management Systems, Limited Resources and Expertise.

A fundamental challenge for many Vietnamese SMEs is the lack of structured data management systems. Many businesses still rely on informal methods such as spreadsheets or paper records, which leads to inefficiencies, errors, data duplication, and an increased risk of data loss. The absence of integrated data systems further limits SMEs' ability to process large volumes of data effectively, hampering strategic decision-making and customer insights. Disorganized storage, inconsistent formats, and weak security frameworks leave businesses vulnerable to data breaches and regulatory non-compliance.

Resource constraints also prevent many SMEs from investing in advanced data management systems or hiring skilled IT and cybersecurity personnel. The 2024 Cybersecurity Summary Report highlights that 20.06% of organizations lack dedicated cybersecurity staff, while 35.56% have no more than five personnel assigned to cybersecurity, which is far below the necessary levels to manage growing digital threats. Addressing these challenges requires clearer regulatory guidance, financial support, and increased investment in cybersecurity infrastructure to help SMEs comply with modern data protection laws and strengthen digital security resilience.



To ensure cybersecurity, organizations must adopt the 24/7 Security Operations Center (SOC) monitoring model, which consists of 3 shifts and 4 teams. Each organization requires a minimum of 8 to 10 dedicated positions. A lack of personnel results in an overload of managing risks and reduces the effectiveness of response and mitigation efforts during incidents. This situation makes organizations more susceptible to cyberattacks, leading to significant financial and reputational damage. Consequently, many businesses neglect data security or delegate responsibility to employees with limited expertise in data protection best practices. This lack of knowledge, combined with insufficient training for current staff, often results in the mishandling of sensitive customer and business data. Without adequate staff training or professional guidance, data protection measures are frequently overlooked, leaving businesses vulnerable to potential data breaches and legal issues related to non-compliance.

II. HOW THE NEW DATA LAWS COULD CHANGE THE GAME FOR SMALL BUSINESSES

The new data protection regulations, including Decree No. 13/2023/ND-CP on Personal Data Protection and Data Law No. 60/2024/QH15, not only impose stricter requirements but also create numerous opportunities to transform how SMEs manage and protect their data.

- **Enhancing Security and Reducing Data Breach Risks;**
- **Expanding International Business Opportunities;**
- **Support from Government and Business Associations for SME Data Protection Compliance.**

II. HOW THE NEW DATA LAWS COULD CHANGE THE GAME FOR SMALL BUSINESSES

1. Enhancing Security and Reducing Data Breach Risks

Implementing personal data protection measures under the new Data Law allows SMEs to mitigate security risks and safeguard customer information. The adoption of advanced security technologies helps prevent cyberattacks, data leaks, and misuse of personal data, ensuring business continuity and regulatory compliance. The law imposes strict penalties, including fines of up to 5% of annual revenue, as outlined in the Draft Decree on administrative sanctions for cybersecurity violations. Following these regulations not only reduces legal and financial risks but also protects brand reputation and fosters customer trust. Furthermore, compliance encourages SMEs to embrace advanced security technologies, enhancing their cyber resilience and improving operational efficiency over time.

2. Expanding International Business Opportunities

One of the key advantages of the new Data Law is its role in facilitating SMEs in accessing international markets more effortlessly. Compliance with data protection regulations builds trust among domestic customers and boosts SMEs' capacity to collaborate with global partners – particularly in locations like the European Union (EU), where adherence to the General Data Protection Regulation (GDPR) is required. Similar regulations in other countries further highlight the significance of data security in global business operations. Meeting international data protection standards enables smooth participation in trade agreements and broadens market opportunities, thereby increasing revenue streams. In an era of globalization and rapid e-commerce growth, regulatory compliance is not just a legal requirement but also a competitive edge that ensures SMEs can succeed in cross-border transactions. By prioritizing data security, SMEs reduce legal risks, enhance their brand reputation, and build credibility with customers and business partners. This strategic compliance approach not only boosts competitiveness but also promotes long-term innovation, resilience, and sustainable growth in an increasingly digital global economy.

II. HOW THE NEW DATA LAWS COULD CHANGE THE GAME FOR SMALL BUSINESSES

3. Support from Government and Business Associations for SME Data Protection Compliance

To help SMEs comply with the new data protection regulations, the government and business associations have launched several support programs designed to ensure regulatory adherence and enhance data security measures.

- **Free Training Programs**

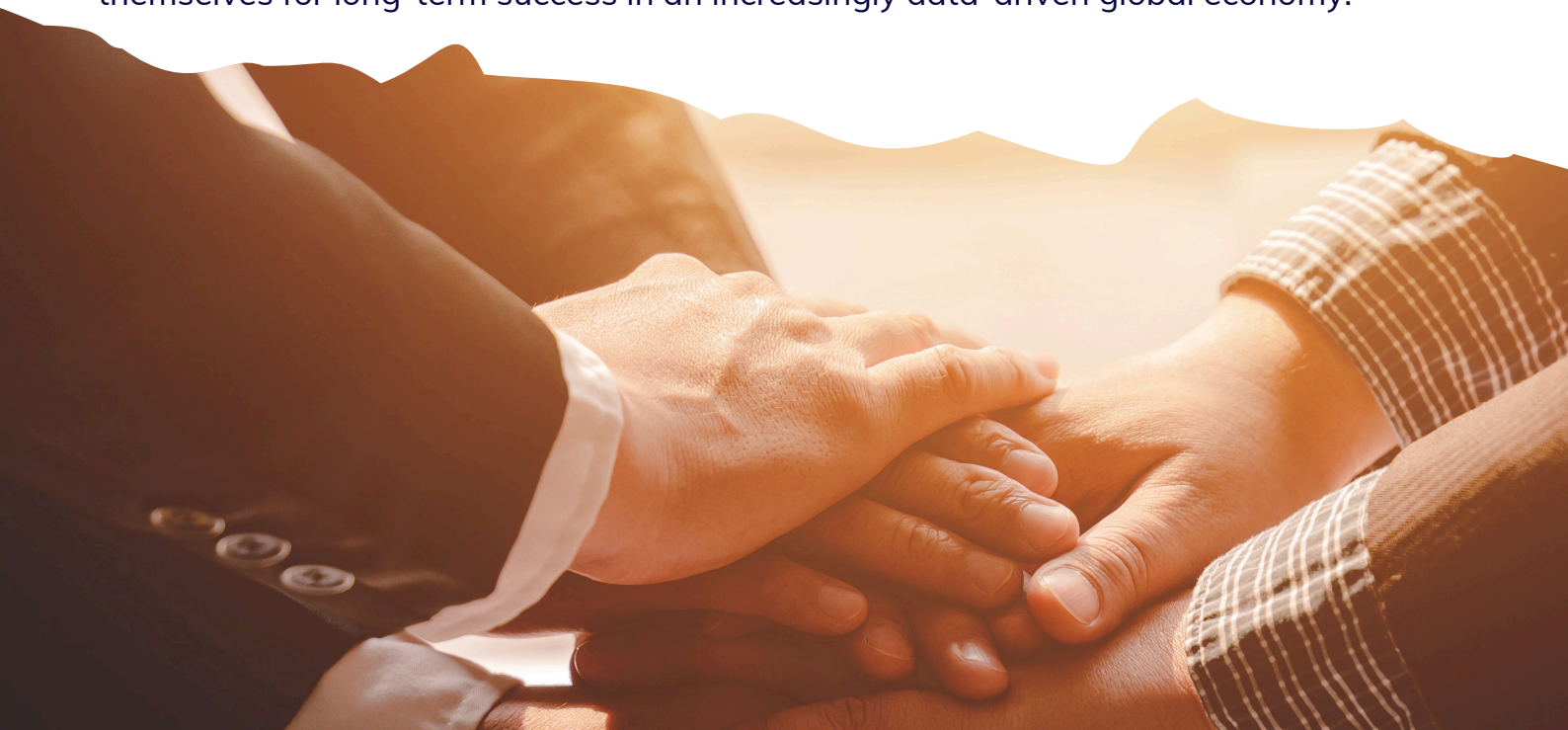
The government and various business associations offer free training programs to equip SMEs with essential data protection skills and knowledge. These sessions cover key topics such as data encryption, access management, and cybersecurity best practices, helping SMEs mitigate risks and enhance data security.

- **Technical Support and Guidance**

Organizations such as the Vietnam Chamber of Commerce and Industry (VCCI) and the Vietnam E-Commerce Association (VECOM) provide technical support through guidance documents, tools, and comprehensive instructions for implementing data protection measures. These resources help SMEs navigate regulatory requirements and adopt practical security solutions without needing extensive expertise.

- **Building a Strong Compliance Framework**

The collaborative efforts of government and business associations create a comprehensive support system that enables SMEs to confidently meet compliance obligations. By leveraging these resources, training programs, and technical assistance, SMEs can safeguard customer trust, enhance operational security, and position themselves for long-term success in an increasingly data-driven global economy.



III. WHAT SMES NEED TO DO TO COMPLY WITH DATA PROTECTION LAWS AND ENSURE BUSINESS OPERATIONS?

To effectively comply with data protection laws, SMEs must adopt a comprehensive data protection strategy that includes legal, technical, and procedural measures. Below are key actions SMEs should take to ensure compliance and enhance their data security resilience:

Establish Clear Data Protection Policies	• SMEs should develop and document a formal data protection policy that outlines procedures for collecting, processing, storing, and sharing personal data. • Ensure that policies align with Decree No. 13/2023/ND-CP on Personal Data Protection and Law No. 60/2024/QH15 on Data to prevent legal violations. • Appoint a Data Protection Officer (DPO) or designate a compliance lead to oversee the implementation of the policy and ensure regulatory adherence.
Conduct Employee Training & Awareness Programs	• Regularly train employees on data privacy regulations, security protocols, and potential cyber threats. • Implement role-based training to ensure that employees understand their responsibilities regarding data handling. • Enforce strict access controls to limit data exposure to authorized personnel only.
Invest in Security Technologies	• Deploy encryption software, firewalls, and secure storage solutions to safeguard sensitive data against cyber threats. • Implement multi-factor authentication (MFA) and intrusion detection systems (IDS) to block unauthorized access. • Regularly perform cybersecurity risk assessments to pinpoint vulnerabilities and take corrective measures.

III. WHAT SMES NEED TO DO TO COMPLY WITH DATA PROTECTION LAWS AND ENSURE BUSINESS OPERATIONS?

Maintain Compliance with Legal Updates & Government Coordination	• Monitor legal updates from the relevant authority. • SMEs should engage with business associations like VCCI and VECOM to stay updated on compliance guidelines and best practices. • Coordinate with regulatory authorities for regular audits and seek legal advice when necessary.
Implement Data Breach Response & Security Audits	• Develop a data breach response plan to quickly address and mitigate incidents in the event of cyberattacks. • Conduct regular security audits and penetration tests to ensure systems remain secure. • Establish a data retention and disposal policy to manage the secure lifecycle of personal data.
Leverage Government & Industry Support Programs	• Leverage government-funded cybersecurity initiatives, such as training programs and financial incentives for digital transformation. • Apply for favorable loans or grants provided by business associations to assist SMEs in investing in cybersecurity infrastructure.

By actively implementing these measures, SMEs can ensure they comply with Vietnam's data protection laws, minimize legal risks, and foster trust with customers and partners. A robust data security framework will not only safeguard business operations but also open doors for international market expansion.

QUOC & ASSOCIATES

We hope this Legal Insights will bring useful information to Clients and readers. For specific advice and more detailed information, please contact us via the contact information listed at the end of this Legal Insights.

If you have any questions and comments on this Legal Insights, please contact:

Hai Thanh Nguyen
Partner

T: +84 94 651 8259
E: hainguyen@quoclaw.vn

Yen Tien Quang Nguyen
Associate

T: +84 82 523 0998
E: yennguyen@quoclaw.vn

Quoc & Associates Law Firm
No.1 Tran Khanh Du Street, Tan Dinh Ward, District 1, Ho Chi Minh City, Vietnam.

www.quoclaw.vn

T: +84 985 036 774

Q&A | QUOC & ASSOCIATES