VNETWORK
safe and saved

LEADING CLOUD SECURITY

VNETWORK
safe and saved

VNETWORK adheres to the Personal Data Protection Decree 13/2023/ND-CP (PDPA)

Overview about decree NO.13 of the government

Promulgated on July 1, 2023, Decree 13/2023/ND-CP signifies a crucial step towards protecting personal data in Vietnam. This decree aims to not only safeguard the rights of individuals and organizations but also to provide support for the lawful and secure processing of personal data. The decree's applicability extends to all entities, encompassing both domestic and foreign organizations and individuals, whenever they engage in the handling of personal data within Vietnam's jurisdiction. This applicability remains valid even in instances where such processing transpires outside the nation's borders.

Specifically, Decree 13/2023/ND-CP regulates the rights of data subjects, the obligations of organizations and individuals processing personal data, principles of personal data protection, measures for personal data protection, and provisions on the responsibilities of state agencies in protecting personal data.

Entities involved in the processing of personal data within Vietnam must duly heed the requirements outlined in Decree 13/2023/ND-CP, which safeguards the rights of data subjects and ensures lawful and secure processing activities.

Decree 13/2023/ND-CP (Personal Data Protection) outlines various personal data types requiring protection, including

General personal data: Comprises personal identification information, encompassing full names, dates of birth, phone numbers, identification document numbers, bank account details, and similar data.

Sensitive personal data: Comprises data concerning sensitive personal attributes, such as political views, religious beliefs, health conditions, and similar characteristics.

Responsibilities of involved parties

Decree 13/2023/ND-CP on Personal Data Protection (PDPA) clearly outlines the roles and responsibilities of all stakeholders throughout the lifecycle of personal data.

Responsibilities of data subjects
(individuals whose data is being processed):

- Provide complete, accurate, and up-to-date personal information to the data controller.
- Request the data controller to provide, correct, delete, or cancel personal information.
- Request compensation from the data controller for damages in case of violations of personal data protection regulations.

Responsibilities of the data controller
(organization or individual determining the purpose and means of personal data processing):

- Define the purpose and means of processing personal data.
- Collect and process personal data by the defined purpose and means.
- Ensure the security of personal data.
- Fulfill other obligations as stipulated by Decree 13.

Responsibilities of the data processor
(organization or individual processing data on behalf of the data controller through a contract or agreement):

- Process personal data by the purpose and means defined by the data controller.
- Ensure the security of personal data during processing.
- Do not use personal data for purposes other than those defined by the data controller.
- Fulfill other obligations as stipulated by Decree 13.

VNETWORK
safe and saved

Implementing Measures for Personal Data Protection

Decree 13/2023/ND-CP outlines various measures to safeguard personal data, including:

01 Measures undertaken by organizations or individuals involved in processing personal data

- Define the purpose and scope of processing personal data.
- Collect and process personal data by the defined purpose and scope.
- Ensure the security of personal data during processing.
- Implement necessary measures to protect personal data from unauthorized access, use, disclosure, copying, alteration, destruction, loss, contamination, interruption, disruption, or other unlawful processing.
- Implement necessary measures to ensure the integrity, accuracy, and currency of personal data.
- Empower data subjects by implementing measures that ensure they can readily access and manage their personal data.
- Ensure compliance with data privacy regulations by implementing comprehensive measures to protect the privacy rights of data subjects.
- Implement appropriate and comprehensive measures to ensure adherence to all applicable legal and regulatory requirements concerning personal data protection.

02 Technical safeguards implemented by organizations or individuals involved in processing personal data

- Throughout the entire lifecycle of personal information, from collection and processing to storage, sharing, use, deletion, and disposal, implement robust information security measures.
- Prioritize the secure transmission of personal information. Implement robust information security measures to protect data during network exchanges.
- Implement information security measures for storing personal information on electronic media.
- Employ information security measures for deleting and disposing of personal information.
- Secure the transmission and exchange of personal information through other communication channels by implementing robust information security measures.

03 State management authorities' actions in upholding this Decree and relevant laws

- Develop and issue regulations, standards, and technical specifications on personal data protection.
- Inspect, audit, and address violations related to personal data protection.
- Provide support, advice, and guidance to organizations and individuals in implementing personal data protection measures.

04 Investigative and judicial measures undertaken by competent state authorities.

These are measures undertaken by competent state authorities to investigate, prosecute, and adjudicate violations of regulations on personal data protection.

05 Other measures as prescribed by law

These personal data protection measures are further detailed in other relevant legal documents.

Why is it necessary to protect personal data?

According to a study commissioned by Apple in 2023*, the total number of data breaches has more than tripled from 2013 to 2022 (from 761 incidents to 2,609 incidents), resulting in the leakage of 2.6 billion personal records in just two years. The situation continued to worsen in 2023, with 1,800 data breaches occurring in the first nine months alone, leaking 1.3 billion personal records.

The report has highlighted several reasons contributing to the increase in data breaches, including

- **The rise in cyberattacks:** This includes ransomware attacks, phishing attacks, and zero-day attacks.
- **The increase in the use of personal data:** This includes personal data stored in the cloud, used in mobile applications, and employed in business operations.

Ensuring the security of personal data is of the utmost importance

If personal data is compromised, misused, or unlawfully disclosed, the consequences can be devastating. This can include

Significant reputational damage

Individuals may experience a breakdown in trust in institutions, potentially impacting their employment prospects, educational opportunities, and social interactions.

Financial ruin

Data breaches put individuals at significant risk of falling victim to fraud, theft, or even exploitation for other criminal activities.

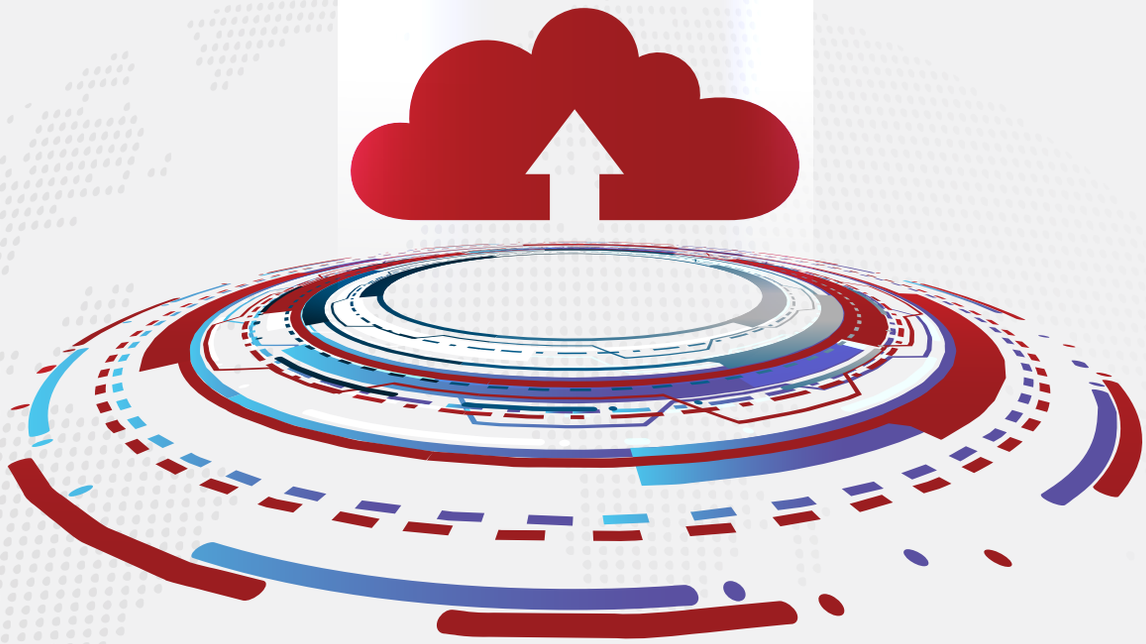
Cyberattacks

Data breaches expose individuals to the risk of having their information stolen and misused for malicious purposes.

Therefore, both individuals and organizations must actively engage in protecting personal data. Individuals need to increase their awareness of the risks associated with data breaches and take appropriate measures to safeguard their personal information. Similarly, organizations entrusted with processing personal data have the responsibility to implement robust measures to ensure its protection.

** According to the report "The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase" conducted by Professor Dr. Stuart Madnick of the Massachusetts Institute of Technology, authorized by Apple and published in December 2022.*

VNETWORK
safe and saved



Cloud technology plays a crucial role in safeguarding personal data

Cloud technology, a method of storing and processing data over the internet, empowers organizations and individuals with the ability to access information from any location, at any time. This technology offers numerous advantages for safeguarding personal data, including

Enhanced data security

Cloud technology utilizes advanced security measures, including encryption, multi-factor authentication, and security monitoring, to protect data from intrusion, misuse, or unauthorized disclosure.

Improved data resilience

Cloud technology allows data to be stored across multiple servers, reducing the risk of data loss due to natural disasters, technical failures, or malicious activities.

Enhanced scalability and adaptability

Minimize the impact of system and data breaches by providing flexible security based on the organization's risk profile.

While cloud technology offers a multitude of benefits for safeguarding personal data, it is crucial for organizations and individuals to be mindful of inherent risks. Mitigating these risks requires selecting reputable cloud service providers with a proven track record of data protection expertise and capabilities. Additionally, implementing robust measures at the organizational and individual level, such as

- Employing robust security measures, including encryption, multi-factor authentication, and continuous security monitoring, is crucial.
- Sharing personal data only with trusted parties.
- Reviewing the security policies of cloud service providers before using their services.

VNETWORK
safe and saved

Enhancing personal data protection capabilities with VNETWORK CLOUD

VNETWORK CLOUD leverages a robust infrastructure to deliver exceptional performance and data security. Located in Tier III international standard data centers across the country, VNETWORK CLOUD utilizes a combination of cutting-edge technologies. This includes NVME+ SSD high-speed hard drives and the latest generation AMD/Intel CPUs to power a robust virtualization server platform. The result? Unmatched uptime of 99.99% and significantly optimized transfer speeds (Read: 53,000+ IOPS, Write: 17,900+ IOPS).

Elevate your business operations with VNETWORK CLOUD solution, unlocking a suite of powerful benefits, including:

Comprehensive data security measures

Comprehensive data security with superior backup processes and data backup mode: 3 days/time. Specifically, backup files are stored in 3 copies with 1 full backup within the last 7 days.

Fortified security measures

Powerful DDoS protection features are integrated right from the start of deploying the Cloud Server solution, enhancing protection and stability for businesses when in use.

Boosting performance and efficiency

VNETWORK CLOUD utilizes NVME+ SSD high-speed hard drives to ensure service uptime rates of up to 99.99%. Additionally, with network speed tests of up to 10Gbps, VNETWORK's Cloud Server solution offers unlimited high-speed bandwidth for data transmission.

Cost and resource optimization

VNETWORK implements flexible payment policies based on actual usage needs (only paying for resources used), helping to save operating costs and resources for businesses.

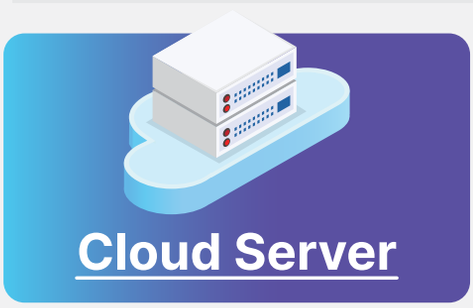
Customer service quality assurance

VNETWORK CLOUD is committed to ensuring the highest level of service quality (SLA), guaranteeing to meet all business requirements for service quality and performance.

24/7 global support

With a team of experienced technology experts who provide unwavering 24/7 support, ensuring your queries and concerns are addressed promptly and comprehensively.

VNETWORK Cloud solutions



Cloud Server

Cloud Storage S3

Cloud WAF

To receive detailed consultation and pricing, please contact VNETWORK at Hotline: **+84 (028) 7306 8789** or email **contact@vnetwork.vn.**

VNETWORK JSC

Floor 23, UOA Tower, 06 Tan Trao, Tan Phu Ward, District 7, City. Ho Chi Minh Vietnam

111 North Bridge Road #17-06 Peninsula Plaza Singapore

contact@vnetwork.vn

+84 (28) 7306 8789

www.vnetwork.vn