DOI: 10.23977/ieim.2023.061018
ISSN 2522-6924 Vol. 6 Num. 10

A Practical Study on Safeguarding Government Data Security

Peng Xing

Guangzhou Municipal Market Supervision & Administration Data Application Center, Guangzhou, Guangdong, 510630, China

Keywords: Digital Government, Government Services, Data Security Governance, Data Sharing, Government Services

Abstract: In the context of the data-driven era, big data has begun to showcase its economic and social value. Meanwhile, the big data technology, as a representative of emerging technologies, will also provide new opportunities and possibilities for government service reform. As an important part of maintaining data openness and ensuring data security, the government should not only protect the security of sensitive data, but also quickly implement data security protection without changing existing business processes, effectively controlling costs, and reducing complexity and risks. This paper highlighted the actual data security governance of government in our organization, including analyzing the nowadays status quo of digital government data security management as well as the demands on such security management, learning about the latest data security governance theory and relevant research results in China and other countries. In addition, this paper proposed countermeasures applicable to our data security governance based on relevant policies, laws and regulations, by which effective prevention and control practices for data security protection has been implemented.

1. Introduction

Data, functioning as key factor[1] in social production, have been widely known by our society, and have deeply impacted the development of diversified industries, including government services. In order to safeguard the data security, a series of related laws and regulations have been enacted one after another in recent years by China government. The concerns on government service system with massive citizen’s personal information and key data of the nation have been significantly focusing on by different local governments nowadays, in consideration of how to ensure the compliance of government service data security. Regarding the requirements on compliance supervision for government service data security, the China State Council has also clearly pointed out that the responsibilities undertaken by person in charge and supervision agent shall be implemented, constructing a full security safeguarding system for digital government[2].

2. Status Quo on Data Security in Government Service Supervision and Administration

In China, the local governments have accumulated massive data in the process of their job performance. In the process of fully facilitating the strategy of "Digital China" and Digital Government, the key factors on data production are playing an increasingly significant role, which has been deemed as the core resources of digital government. However, in recent years, the divulgence event due to hacker attack from external world, illegal pilfer are increased day by day. Meanwhile, in the process of data being shared and opened up to publics among different departments, different platforms and different fields, which means there must be more security risks to be faced.

2.1 Features of government service data

1) Higher sensitivity

The government service data involves in public security, national policies, personal privacy and so forth, full of higher sensitivity, which relates to the economy of a nation and the daily life of people. If such data are stolen, damaged or changed by criminals, it will seriously impact the credibility and reputation of government, meanwhile, it will be a threat to personal privacy or even the national security and the stable society[3].

2) Differential data applicable scenario

The process of government service data involves in diversified application scenarios such as different agencies and bodies, off-line/on-line business modes. The requirements on compliance and data governance modes for data processing to be followed under different service scenarios and different purposes are different[4].

3) Multiplex modeling heterogeneous

The data for government service supervision are from different channels, different levels, different systems, in which the standards for such data are basically unified, but quite difficult to be governed due to its complicated logic.

4) Frequent data exchange

The government service data are associated with all social activities, which are collected by government agencies for diversified business and service scenarios, in addition, such data are frequently exchanged in different modes among different agencies.

2.2 Main issues on data security

1) Data security management agencies and systems are not available

In the traditional government service supervision procedures, many agencies have no data security management office because of data security being ignored and relevant data security management systems compatible with administrative supervision were not available. The main representation is that the personal information and data security protection, data interface security control strategies, data interface security specifications, data asset security management and other institutional systems are insufficient, because of which the rules and regulations for relevant personnel are not followed when they are proceeding daily data processing work, easily resulting in situations such as excessive authorization for data operations so that leads to data exposure or divulgence.

2) Insufficient countermeasures for safeguarding data security

Before the data was called by government service offices, countermeasures are not available for data security due to lack of awareness of data protection. The main representation is that the authentication for user who requests calling the data is not proceeded or specific address access through technical means is not restricted before calling the data; no approval procedures available for the data calling and no interface log audits available within regular period, and no data security audits available for such logs at different stages of data processing activities.

3) Data assets identification and category was ignored

Many government service agencies, because of their concerns on system functionality for long-term, always neglect the sort, classification and protection of data. The main representation is that the data asset security management system is not available, data classification standards are not available, and no sorting for data assets. The protection for internal data of an organization will be chaos because of insufficient data classification and sort, which is not conducive to the subsequent control of data.

4) Data risk monitoring system was not available

Most government departments are unable to timely monitor risks on data security because of insufficient risk monitoring system. In case of any data security event, they may not be able to timely handle with. The main representation is that a data security risk monitoring and warning mechanism is not available, no normalized data security risk monitoring platform available, and no a data security risk closed-loop management mechanism available.

5) Data security training plan was not available or proceeded

Most staff in government agencies have no awareness of data security. The main representation is that the data security training plans are not available, no regular data security education and training for relevant practitioners, and no data security training organized for staff.

2.3 Difficulties on government service data security management

● The frequent changes in the data asset ledger make it difficult to update information in a timely manner, and the identifiability of data security risks is insufficient.

● The partition for rights and responsibilities related to data security is not clear enough, and staff in different jobs have no sufficient awareness on responsibilities of data security, or lower awareness on data security.

● The data security regulation is difficult to be implemented, and significant differences between control measures and actual implementation are existing [5].

● Poor communication during data security operations impacts the emergency response decision and execution.

3. Theoretical Support System for Data Security

3.1 Guideline for Policies and Laws & Codes

In recent years, the Ministries of central government and local governments have intensively enacted multiple policies and regulations for data security (see Table 1), for reinforcing relevant safeguard system. In addition, the China State Council and Ministries have also enacted many related policies and regulations for data security in 2021, such as the Key Information Infrastructure Security Protection Regulations issued on July 30, 2021 and implemented on September 1, 2021, the Network Security Review Measures issued on December 28, 2022 and implemented on February 15, 2022, and the Management Measures for Transportation Data Sharing in Government Service issued on April 6, 2021.

In addition to those enacted by State Council and Ministries, many local governments have also enacted some local data related regulations in 2021. For example, Beijing issued the Beijing Public Data Management Measures, Shanghai issued the Shanghai Data Regulations, and Guangdong issued the Guangdong Provincial Digital Economy Promotion Regulations on July 26, 2021.

In 2023, the Office of Cyberspace Administration the Guangzhou Municipal Party Committee issued the Guidelines for Network Data Security Work of Guangzhou, and the Guangzhou Municipal Digital Administration successively issued the Management Measures for Government

Data Security of Guangzhou and the Overall Plan for Government Data Security of Digital Government Service of Guangzhou (2023-2025).

The laws and regulations on data security mentioned above have provided a solid theoretical basis for implementing the Implementation Measures of the CPC (Party Group) Network Security Responsibility System, the Guiding Opinions of the State Council on Strengthening the Construction of Digital Government, and the Reform Plan for the Unified Basic Operation and Maintenance Management of Guangzhou Digital Government, which accelerates the construction of a comprehensive security safeguard system for digital government by Guangzhou government service departments, and comprehensively strengthening the responsibility of digital government security management[6].

Table 1: Relevant Policies and Laws for Data Security

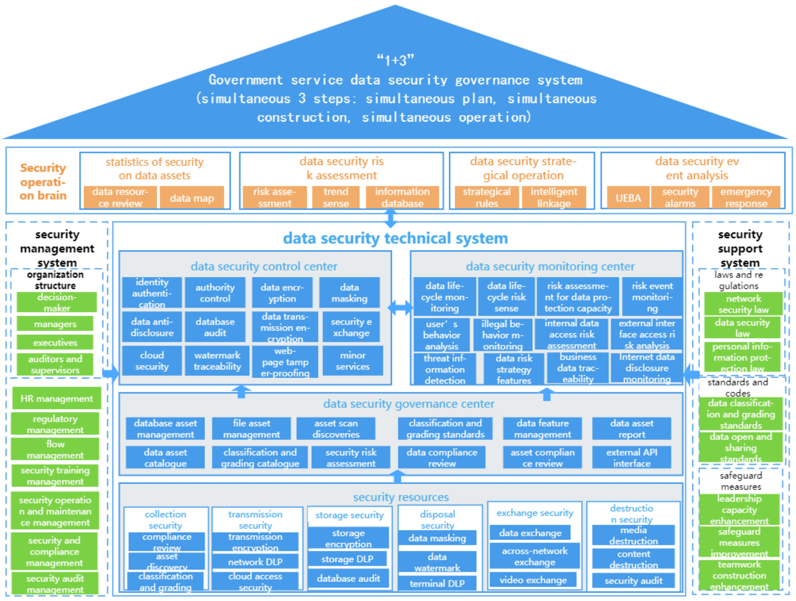
Promulgated Year	Policies and Laws	Data Security Description Involved
2021	Data Security Law of the People's Republic of China	This Act fills up the legal gap in the field of data security protection in China, and it provides legal supports for safeguarding data security and maintaining data sovereignty in China.
2021	An Outline of the 14th Five-Year Plan for National Economic and Social Development of the People's Republic of China and the Vision Goals by 2035	This Act strengthens the data protection, involving in national interests, trade secrets, personal privacy and other data, and improves the security protection capability for data resources throughout their entire lifecycle
2022	The 2022 Government Work Report	This report proposed that we are required to strengthen cyberspace security, data security, and personal privacy protection, and improves the national security system and construction capacity.
2022	Measures for the Management of Data Security in the Field of Industry and Information Technology (Trial)	This Act proposed that it is required to create a risk monitoring mechanism for data security and to develop monitoring and warning interfaces as well as relevant standards
2023	The 2023 Government Work Report	This report proposed that we shall promote a deep integration between the digital economy and the real economy, vigorously develop the digital economy, and strengthen network, data security, and personal privacy protection. The statement on data security and personal privacy protection has been written in the government report for consecutive three years.
2023	Overall Layout Plan for the Construction of Digital China	This plan required that we shall enhance data security capabilities, establish a fundamental system for data classification and sorting protection, and improve the network data monitoring, warning, and emergency response system

3.2 Theoretical guideline for data security governance

In January 2023, at the 2nd Data Security Governance Summit, the "Data Security Governance Practice Guide (2.0)" was officially released, summarizing the "3344" practice mode for data security governance (Note: 3344 refers to 3 goals +3 systems+ 4 dimensionalities +4 routines). This mode sets three goals for governance and divides the governance system into three stages, and four dimensions for governance, and practicable in four steps, which provides optimized practices and blueprint planning related to data security governance construction. Meanwhile, in May, the Data Security Governance Professional Committee of the Network Security and Information Industry Alliance released the White Paper for Data Security Governance (V.5.0). This White Paper analyzed the strategic development of China's digital economy and the new situation and trends of data security, clarified the concept of data security governance and interpreted the connotation of data security governance, improved the requirements and framework on data security governance, explained the latest regulatory requirements and technical specifications such as laws, regulations, and standards, comprehensively and systematically introduced the relevant security and technology requirements, tools, and development trends around the data lifecycle, and proposed future prospects and suggestions for data security governance.

4. Systemic Framework for Government Service Data Security Governance

This framework aims at maintaining the security of government data and promoting the orderly developed and utilized data resources, constructing an operation brain for data security and establishing an integrated governance system for government service based on the government network infrastructure environment, three major systems of data security management, technology, and support, expressed as Visible Data, Visible Risk, and Controllable Security, as shown in Fig. 1:



"1+3"
Government service data security governance system
(simultaneous 3 steps: simultaneous plan, simultaneous construction, simultaneous operation)
Security operati-on brain
statistics of security on data assets
data resour-ce review
data map
data security ris k assessment
risk asse-ssment
trend sense
information database
data security strate-gical operation
strategical rules
intelligent linkage
data security ev ent analysis
UEBA
security alarms
emergency response
security management system
organization structure
decision-maker
managers
executives
auditors and supervisors
HR management
regulatory management
flow management
security training management
security operatio n and maintenan ce management
security and compliance management
security audit management
data security technical system
data security control center
identity authenti-cation
authority control
data encr-yption
data masking
data anti-disclosure
database audit
data trans-mission en-cryption
security e xchange
cloud security
watermark traceability
web-page tamp er-proofing
minor services
data security monitoring center
data life-cycle mon-itoring
data life-cycle risk sense
risk assessme-nt for data pro-tection capacity
risk event monitori-ng
user' s behavior analysis
illegal be-havior m-onitoring
internal data access risk assessment
external inter face access ri sk analysis
threat inf-ormation detection
data risk strategy features
business data trac-eability
Internet data disclosure monitoring
data security governance center
database asset management
file asset management
asset scan discoveries
classification and grading standards
data feature management
data asset report
data asset catalogue
classification and grading catalogue
security risk assessment
data compliance review
asset complian ce review
external API interface
security resources
collection security
compliance review
asset discovery
classification and grading
transmission security
transmission encryption
network DLP
cloud access security
storage security
storage encryption
storage DLP
database audit
disposal security
data masking
data watermark
terminal DLP
exchange security
data exchange
across-network exchange
video exchange
destructio n security
media destruction
content destruction
security audit
security support system
laws and re gulations
network security law
data security law
personal info-rmation prot-ection law
standards and codes
data classificat-ion and grading standards
data open and sharing standards
safeguard measures
leadership capacity enhancement
safeguard measures improvement
teamwork construction enhancement

Figure 1: Data Security Governance System Framework

4.1 To set up a technical system for data security

The technical system for data security refers to an active defense by modern information technologies to protect data throughout its entire lifecycle.

1) Security on Data Collection

In consideration of characteristics of unstructured, massive, and dispersed government data, by using keywords, regular expressions, and other intelligent technologies such as natural language processing and machine learning clustering classification are introduced to achieve intelligent classification and grading of data. In subsequent security control, fine-grained security strategies are matched based on the classification and grading results, for a final goal of "highlighting key points and precise protection".

2) Security on Data Transmission

The government big data bureau or government data sharing and exchange platform are required to map the corresponding services to the government extranet for each commission to access services through the government extranet. In order to achieve the security of the access link, some system addresses are not convenient for public disclosure, that’s why it is necessary to use link encryption and proxy addresses for secure access. By providing a secure access mechanism based on transmission encryption through a secure access gateway and using proxy technology and TLS connections to provide secure services, it is able to process remote users' access requests to internal network services by rewriting links and ports, and use national encryption algorithms for link data encryption to reduce network exposure and protect internal networks from attacks and divulgence of internal resources. Meanwhile, the DLP technology is used to prevent illegal data divulgence from network channels, and the approval function is available for the normal needs of file export.

3) Security on Data Storage

Government data is often stored in servers, databases, clouds, office terminals in a centralized or decentralized manner. Technical means such as data encryption, data safes, terminal DLP, storage DLP, cloud access security agents CASB, database auditing, etc can be stored in encrypted form, authorized to be decrypted and used by corresponding users according to classified and graded control permissions to prevent unauthorized access by cloud service providers and third-party operation and maintenance operators, even divulgence of data, setting up prior identity authentication and a full process security system with contingency management and post audit management. Meanwhile, with the promulgation of the Data Security Law, regulatory agencies such as cybersecurity and public security have gradually made data security reviews the main content of security inspections. By conducting compliance checks and self-inspections on security, they ensure that the storage of important data meets security regulatory requirements.

4) Security on Data Processing

Abundant scenarios are available for using government data. With the promotion of opened sharing of government data, data convergence, integration and utilization among departments, levels and regions continue to deepen. In particular, with the popularization of "Internet + government services", "mobile government", "request at most once" and "One Network for Everything ", the security risks of government data in the process of processing are increasingly obvious. By using technology such as application protection, data desensitization, and watermark tracing, data security can be achieved in various business and service systems, office terminals, and other scenarios, preventing data from being illegally downloaded, deleted, tampered with, or abused, for a purpose of protecting personal privacy information security.

5) Security on Data Exchange

The government extranet and Internet area nowadays are usually isolated by gateways, but this simple data exchange cannot meet the new demand of "Internet + government services", resulting in the limited business service capacity of government agencies, especially to the publics. If we bypass network gates or switch to firewalls for business or service, it is not only non-compliance, but also reduce the security between network regions. Through a secure data exchange system, it is able to proceed various types of data, files, and videos for securely exchanging data between internal and external networks, as well as across domains so that the data silos formed over the years can be cleared up, and a "bridge tunnel" for cross network business services can be built on the basis of physical isolation, ensuring data security while processing data sharing and exchange.

6) Security on Data Disposal

Regarding to the data security issues associated with the disposal of hardware devices such as the entire computer and various types of storage media, as well as the security needs for expired destruction after highly sensitive data sharing, media destruction (such as physical destruction) and content destruction (such as demagnetization technology and file expiration control) can be used. By process approval and security audit, the data destruction can be ensured to be safe, controllable and post audit, preventing risks caused by malicious data backups and data restoration[7].

4.2 Security on operating brain

The security operation brain collects user behavior data from hardware devices, networks, application systems, etc based on big data technology, and analyzes massive multi-source heterogeneous data through visual modeling technology. It is able to timely discover security alarm events, provide alarm information, and provide security response linkage based on designed activities. It is required to set up an integrated government data security operation system with "visible data, visible risk, and manageable security" from four dimensions, including data assets, security risks, security policies, and security events.

1) Security on Data Asset Management

It includes taking inventory for data assets and business, identification of important assets, including sorting out key business scenarios, business access relationships, status quo of security etc. In order to make up for the shortcomings and strengthen the foundation, it is required to prepare for basic security and protection.

2) Data Security Strategical Operation

It is required to define access and protection strategies for data security associated with data assets and visitors, and implement data security supervision strategies synchronously in diversified scenarios to ensure policy consistency and effectiveness.

3) Data Security Risk Assessment

The risk assessment on data security supervision aims to achieve the value protection of data assets and ensure the safe flow for data assets on the data value chain. It evaluates the security risks faced by data assets from four dimensions, i.e time, space, management, and technology, and designs a risk control mechanism for data security supervision. It is required to solve key issues such as "dark assets, disclosure, and vulnerability" [8].

4.3 Support System for Data Security Management

The technical and support system is used to implement relevant work through the data security management system and support system. It includes classification and grading, system planning, organizing the governance of data assets through business systems, identifying sensitive data, and completing data classification and grading; By identifying the access relationship between data subjects and objects, sorting out data access permissions, drawing data flow, it is able to develop relevant systems, standards, processes, etc. Through the operation system composed of data security brain, management system, and technology platform, the security strategies are controlled based on business data and risk situations, to achieve data asset monitoring, data flow monitoring, monitoring and analysis, timely visual of security events, and audit traceability to achieve overall monitoring of data security.

5. Practice on Safeguarding Government Data Security

The construction of a data security system is never achieved overnight, never be successful once for all. The data security system takes the safe application of user’s data assets as its vision, uses independent and controllable data security technology means and products, and constructs a data security governance system associated with the entire data lifecycle under phased construction.

Following is the steps for practice:

By data security governance, it is able to analyze the current status of user data assets, develop organizational structures, institutional processes, personnel training plans, etc. for customers, prepare the plan and feasibility study for the technical support construction of data security around the entire data lifecycle, setting up a data security technology protection system that meets the needs of real scenarios.

In consideration of the existence of information silos between various information security modules, it is often unable to achieve a perfect linkage so that generates some pain points in data security management, detection, protection, and traceability during the operation phase. Through sustainable operation, it is helpful to users clearing up the silo effect between various information security modules, solving the above-mentioned pain points, and combining UEBA situational awareness technology to achieve security reinforcement, continuous optimization, cost reduction and efficiency increase.

The data security governance system, based on personnel organization, technical support and strategic norms, plays an effectively role in protecting government data throughout its lifecycle.

The data security governance system and methodology proposed in this paper are currently being preliminarily promoted in our organization, for a purpose to achieve overall data security through specialized data security governance planning, comprehensive data security protection on government internal and external network terminals, reducing the probability of security incidents such as disclosure by internal staff and unintentional disclosure, as well as the negative impact caused by them. The NLP, UEBA and other technologies used in the project will significantly reduce the missed and false alarm rates of sensitive data identification, improve the recognition of category, and achieve classification and classification accuracy and efficiency, exceeding the traditional method by 50%. 382 servers deployed on both the government external network and the government internal network in our organization, both of which require the deployment of anti-disclosure systems. Followed by we will gradually strengthen our security protection strategies and controllable scope.

The security system is highly compatible with the Data Security Law, by which it has clarified the main responsibilities of data security protection, guided data managers to fully integrate their own situation and regulatory requirements, fully learnt about the main problems, behaviors, and scenarios currently facing so that is able to cope with the current open and complicated security environment. The project fills the gap in data security governance and strong replicability is available, enabling rapid promotion and deployment to other government departments.

6. Conclusions

This paper summarized the current situation of data security in the government affairs (including security trends, security characteristics and regulatory difficulties), and combined relevant national policies, laws and regulations, standards and codes, data security governance theories, for a purpose to set up a data security regulatory system for medical industry. Meanwhile, depending on our own data security practices, we have clarified data assets, achieved data classification and grading, comprehensively evaluated data security risks, constructed a long-term mechanism for data security operation, and strengthened data security defense lines. This has also provided reference significance for other government service agencies' data security supervision, so as to jointly maintain a perfect environment for data security.

References

[1] HU Guohua, WANG Zhendong, LIU Shaoyu, et al. Analysis and Innovative Practice of Government Data Security Compliance [J]. Information and Communication Technology and Policy, 2023, 49 (02):20-29

[2] Guiding Opinions of the State Council on Strengthening the Construction of Digital Government [EB/OL] (2022-06-23)[2022-08-28].https://www.gov.cn/zhengce/content/2022-06/23/content_5697299.htm.

[3] ZHENG Pan, CHEN Chen, MA Yang, et al. Construction of Data Security Management in Medical and Health Institutions [J]. China Digital Medicine, 2023, 18 (01):7-11.

[4] WANG Tiangang, LI Xiaoliang, WEI Rong, et al. Ten Year Practice of Building a Comprehensive Protection System for Hospital Data Security [J]. China Digital Medicine, 2022-17 (08):1-8.

[5] NIU Wei, LIU Huze. Study on Data Security Management Strategies in Medical Institutions [J]. Network Security Technology and Applications, 2022, (10):105-107.

[6] Data Security Governance Practice and Guideline (v 2.0) officially enacted by data security promotion plan, https://baijiahao.baidu.com/s?id=1755152205564522495&wfr=spider&for=pc, 2023,1,16

[7] ZHOU Nuanqing. Construction and Practice of Data Security Supervision System in the Medical Industry [J]. Fujian Computer, 2023,39 (09):45-50.

[8] WANG Yu, AN Peng, LI Wenke, et al. A Study and Practice on Government Data Security Governance System [J]. Information Security Research, 2023, 9 (09):900-907.