Postprint: A GDPR-Based Corporate Self-Assessment Indicator System for Personal Data Protection

Authors: Xu Jicang, An Xiaomi, Sun Jiarui, Guojiao Wu, Wang Li

Date: 2023-08-27T00:00:00+00:00

Abstract

[目的/意义]To address the challenges Chinese enterprises face in managing EU-related personal data under the European General Data Protection Regulation (GDPR), establish and improve an evaluative indicator system for personal data protection in China, and promote personal data protection management among Chinese enterprises.[方法/过程]By integrating specific provisions of the GDPR and employing the Analytic Hierarchy Process (AHP) method, we construct a GDPR-based self-assessment indicator system for personal data protection applicable to Chinese enterprises.[结果/结论]The indicator system can meet the basic self-assessment requirements of existing enterprises in response to the GDPR. Additionally, indicators derived from GDPR provisions within the system hold referential value for improving national standards such as the "Information Security Technology - Personal Information Security Specification."

Full Text

Preamble

Research on Self-Evaluation Index System for Enterprise Personal Data Protection Based on GDPR

Xu Jicang[1], An Xiaomi[1,2,3], Sun Jiarui[1], Wu Guojiao[1], Wang Li[1]

[1]School of Information Resource Management, Renmin University of China, Beijing 100872
[2]Key Laboratory of Data Engineering and Knowledge Engineering, Ministry of Education, Beijing 100872
[3]Smart City Research Center, Renmin University of China, Beijing 100872

Abstract

[**Purpose/Significance**] This study addresses the challenges Chinese enterprises face in managing European personal data under the European General Data Protection Regulation (GDPR), aiming to establish and improve China's personal data protection evaluation index system and promote corporate personal data protection management. [**Method/Process**] Combining specific GDPR provisions with the Analytic Hierarchy Process (AHP), we construct a self-evaluation index system for personal data protection based on GDPR applicable to Chinese enterprises. [**Result/Conclusion**] The index system can meet the basic needs of existing enterprises for GDPR self-evaluation. Meanwhile, indicators derived from GDPR provisions in the system offer reference value for improving national standards such as the *Information Security Technology – Personal Information Security Specification*.

Keywords: GDPR; personal data protection; index system; analytic hierarchy process
Classification Number: G203
DOI: 10.13266/j.issn.0252-3116.2018.23.014

Introduction

On April 14, 2016, after four years of deliberation, the European Parliament passed the General Data Protection Regulation (GDPR) [1-2], which took effect on May 25, 2018. As a unified EU law requiring no national transposition, GDPR ensures personal information security across member states. Unlike the 1995 Data Protection Directive (repealed upon GDPR's enactment), this regulation significantly avoids inconsistencies arising from national transposition processes [3]. GDPR also guarantees individuals' control over their information, reassigns obligations and responsibilities between data controllers and processors, and improves special data protection rules for cross-border transfers and criminal activities [4-5].

GDPR represents a major transformation not only for European personal information protection law but also for Chinese enterprises engaged in European data business [6]. Article 2(1) stipulates that GDPR applies to the processing of personal data of data subjects within the EU, regardless of whether the processing occurs within the Union. Additionally, Article 3 states that data controllers and processors within the EU are subject to the regulation regardless of where processing takes place. Consequently, Chinese enterprises handling personal data of EU residents—particularly in communications and big data—face GDPR scrutiny, with non-compliance carrying enormous penalties. GDPR establishes a tiered legal liability system, with Article 83(2) enumerating 11 circumstances for administrative fines and Articles 83(3)-(6) setting maximum penalties. Violations of cross-border data transfer requirements or unauthorized collection and processing can result in fines up to €20 million or 4% of global annual turnover [8], potentially bankrupting many affected Chinese enterprises.

In reality, numerous small and medium-sized enterprises have minimal understanding of GDPR and lack knowledge of compliant personal data management practices.

Simultaneously, GDPR's four-year development process makes it a milestone in international personal data protection legislation. Its innovative conceptual framework achieves compliance through combinations of personnel, process, and product controls. Its definitions of personal data, allocation of data protection officer responsibilities, and management of overseas data offer valuable references. By contrast, China's relevant laws and standards require further refinement. As a general personal data protection law, GDPR leaves considerable interpretive space, with most provisions constituting general principles suitable for adoption and reference. In recent years, China's big data and machine learning technologies have flourished, increasing personal data collection and mining activities and highlighting privacy concerns. Chinese authorities and research institutions have issued guidance and national recommended standards to regulate relevant entities (primarily enterprises), but these standards lack the legal force and practical utility of GDPR. Incorporating beneficial GDPR content while providing an evaluative index system for Chinese standards would incentivize and guide enterprises in personal data protection management, significantly benefiting China's personal data security.

1. Domestic Existing Research

China's first personal information protection system was GB/Z28828-2012 *Information Security Technology – Guidelines for Personal Information Protection in Public and Commercial Service Information Systems*, guided by the Ministry of Industry and Information Technology, drafted by the China Software Testing Center, and issued by the Standardization Administration [9]. Following the 2008 draft *Personal Information Protection Specification*, renamed *Personal Information Protection Guidelines* on May 11, 2010, and further revised on September 23, 2011, the standard took effect on February 1, 2013. It defines roles and responsibilities of data subjects, controllers, recipients, and third-party evaluation agencies across four processing stages: collection, processing, transfer, and deletion [10]. Its most notable feature requires explicit authorization from data subjects before collecting and using sensitive personal information [11]. The standard also proposes eight fundamental principles: clear purpose, minimal necessity, open notification, individual consent, quality assurance, security protection, good faith fulfillment, and clear responsibility.

Since 2014, academic institutions have conducted research on enterprise personal information protection indicators and evaluation. Professor Zhang Ping' team at Peking University's Internet Law Center, in collaboration with the China Science and Technology Law Society, released the latest *Internet Enterprise Personal Information Protection Evaluation Standard* (hereinafter "the Standard") in December 2015 [12], and published consecutive *Sampling Evaluation Reports on Internet Enterprise Personal Information Protection*, establishing a

third-party evaluation-constrained protection system [13]. The Standard uses informed consent, legality and necessity, clear purpose, individual participation, information quality, and security responsibility as basic principles to formulate an index system covering consent, collection, processing, use, transfer, individual participation, policy modification, security responsibility, and special domain personal information [14]. Professor Zhang Ping stated that the Standard aims to operationally advance personal information protection in the internet sector and promote industry self-regulation, enabling enterprises to benchmark their policies and practices against the Standard for timely adjustment.

China's latest personal information security protection system is GB/T35273-2017 *Information Security Technology – Personal Information Security Specification*, proposed by the National Information Security Standardization Technical Committee (SAC/TC260) and drafted by multiple institutions including Beijing Information Security Evaluation Center, China Electronics Standardization Institute, Sichuan University, Peking University, Tsinghua University, Alibaba, and Tencent [16]. As a nationally encouraged recommended standard applicable to "competent regulatory departments, third-party evaluation agencies, and other organizations for supervision, management, and assessment of personal information processing activities," the Cybersecurity Administration explicitly positioned it as a "foundational standard document for China's personal information protection work, laying the groundwork for relevant laws and regulations" [17]. The system aligns with enterprise security obligations under the *Cybersecurity Law of the People's Republic of China*, specifying compliance requirements for personal information collection, sharing, user control, enterprise management systems, and privacy policies of Alibaba and Tencent. It establishes seven principles for personal information controllers: consistency of rights and responsibilities, clear purpose, choice and consent, minimal necessity, openness and transparency, security assurance, and subject participation.

In summary, China has developed at least three standard systems for enterprise personal information protection meeting basic regulatory and evaluation requirements. However, these systems lack corresponding scoring index systems, hindering practical implementation. Moreover, most systems, including Professor Zhang Ping's, pursue comprehensiveness at the expense of specificity, imposing heavy business and financial burdens on enterprises.

2. Evaluation Index Analysis

This index system comprises three layers (see Figure 1 [Figure 1: see original paper]): (1) the target layer assessing enterprise-level personal privacy data protection; (2) the principle layer containing eight important principles derived from integrating core principles of national standards and GDPR, organized according to the personal data security protection process; and (3) the index layer containing 17 practical indicators distilled from a comprehensive review of GDPR, providing important reference for enterprises to assess their GDPR compliance gaps.

The principle layer was selected and merged from GDPR and China's three standard systems based on criteria related to data subjects and data processes, including: clear purpose principle, choice and consent principle, minimal necessity principle, reasonable stewardship principle, subject participation principle, openness and transparency principle, security assurance principle, and self-constraint principle. The first three are fundamental principles mentioned in GDPR, while the remaining five are drawn from China's recommended national standard *Information Security Technology – Personal Information Security Specification* ("China's GDPR").

The clear purpose principle requires that personal data collection be genuinely business-driven with effective documentation and reasonable access rights allocation. The choice and consent principle mandates explicit written declarations for personal data collection; any deliberately concealed consent mechanism is illegal and invalid. The minimal necessity principle requires that collection frequency and quantity satisfy maximum minimization and be directly related to business functions. The reasonable stewardship principle, summarized from GDPR and national standards regarding personal data retention, includes indicators such as retention time minimization, encryption security, record orderliness, database analysis, device management, and data protection personnel independence, aiming to evaluate anonymity, security, and orderliness during retention. The subject participation principle comprises access control, subject requests, and activity traceability during data use, requiring enterprises to grant data subjects rights to modify and delete data while tracing usage activities. The openness and transparency principle applies to data transfer, requiring public assessment of cross-border transfer impacts and consent before transfer, plus feedback solicitation and complaint procedures. The security assurance principle applies to data security disposal, requiring early warning mechanisms to notify regulatory authorities and data subjects, minimizing losses during security incidents, and establishing remediation measures or emergency plans. The self-constraint principle requires effective management of enterprise group structures and contact information throughout the process, personnel control, and appointment of data protection officers based on enterprise size to oversee data processing logic and subject assessment.

The index layer is entirely derived from GDPR provisions, covering all data management stages with strong specificity and sound legal logic, providing concrete measurement for the principle layer. Table 1 provides the meaning and explanation of each indicator.

3. Evaluation Index Weights

This index system divides indicators by personal data management process stage, making indicators mutually independent and suitable for weight calculation using the Analytic Hierarchy Process (AHP). AHP is an important semi-qualitative and semi-quantitative weighting method that collects pairwise importance comparisons through expert questionnaires, calculates geometric means of

indicator scores, and normalizes them to obtain final weights after consistency testing.

In June 2018, this study distributed questionnaires to six experts in information resource management and big data fields. Through careful calculation, we obtained weights for each principle and indicator (see Table 2). The principle weights are shown in column Wi, with a matrix consistency ratio (CR) of 0.0141, far below 0.1, confirming valid weighting results. Analysis of principle-to-target weighting reveals that reasonable stewardship principle, security assurance principle, subject participation principle, and choice and consent principle carry higher weights, indicating expert consensus on their importance in enterprise personal data management.

Through single-level sorting and consistency testing for each indicator relative to its principle (omitted for brevity), we conducted overall hierarchical sorting to obtain final indicator weights (see Table 3). The overall sorting consistency test yielded CR = 0.0386 (<0.1), indicating good matrix consistency. The total sorting column shows the final weighted ranking results, with early warning notification, personal data authorization awareness, and access control degree ranking as the top three indicators.

This study constructs an enterprise personal data management index system that clarifies important GDPR principles and indicators, offering beneficial supplements to relevant national standards. Principles such as reasonable stewardship and subject participation are important principles not yet highly refined or fully described in national standards, while indicators like early warning notification and access control degree provide constructive reference for improving national standards. The index system maintains relative completeness in satisfying national standard principles while proposing targeted indicators for GDPR, proving highly valuable for self-evaluation by enterprises handling EU personal data. Future large-scale surveys will further verify the system's accuracy and effectiveness. Additionally, we will promote personal data protection management through "evaluation-driven improvement," assess the system's social effectiveness, and deepen related research.

References

[1] Gui Changni. Impact and Countermeasures of EU General Data Protection Regulation [J]. China Information Security, 2017(7): 90-93.
[2] EU Congress. General Data Protection Regulation (GDPR) [EB/OL]. [2018-04-14]. https://gdpr-info.eu/.
[3] Office Automation Editorial Department. Coping with GDPR [J]. Office Automation, 2017, 22(16): 17.
[4] Wang Jin. On Improving the Informed Consent Principle in Personal Information Protection—Taking EU General Data Protection Regulation as an Example [J]. Journal of Guangxi Administrative Cadre Institute of Politics and Law, 2018, 33(1): 59-67.

[5] Liu Yun. Development and Reform of European Personal Information Protection Law [J]. Jinan Journal (Philosophy & Social Sciences), 2017, 39(2): 72-84.
[6] Zhang Jianwen, Zhang Zhe. Research on Extraterritorial Effect of Personal Information Protection Law—From the Perspective of EU General Data Protection Regulation [J]. Journal of Chongqing University of Posts and Telecommunications (Social Sciences Edition), 2017, 29(2): 36-43.
[7] He Zhile, Huang Daoli. Background and Impact of EU General Data Protection Regulation [J]. Information Security and Communications Privacy, 2014(10): 72-75.
[8] Peng Xing. Analysis of EU General Data Protection Regulation and Its Implications for China's Credit Supervision in the Big Data Era [J]. Wuhan Finance, 2016(9): 42-45.
[9] National Information Security Standardization Technical Committee. GB/Z28828-2012, Information Security Technology—Guidelines for Personal Information Protection in Public and Commercial Service Information Systems [S]. Beijing: Standards Press of China, 2013.
[10] Huang Zihe. National Standard for Personal Information Security Ready to Launch [J]. China Economic & Informatization, 2012(7): 90-91.
[11] People's Daily Online. China's First National Standard for Personal Information Protection Implemented on February 1 [EB/OL]. [2018-03-21]. http://politics.people.com.cn/n/2013/0121/c1027-20274730.html.
[12] Peking University Internet Law Center, China Science and Technology Law Society. Internet Enterprise Personal Information Protection Evaluation Standard [J]. Internet Law Review, 2015, 17(1): 3-14.
[13] Peking University Internet Law Center, China Science and Technology Law Society. Sampling Evaluation Report on Internet Enterprise Personal Information Protection (2017) [J]. Internet Law Review, 2016(1): 232-240.
[14] Zhang Zhe. Research on Data Portability Right in EU Personal Data Protection Law: Implications and Insights [J]. Journal of Guangxi Administrative Cadre Institute of Politics and Law, 2016, 31(6): 43-48.
[15] Editorial Department. Release of Internet Enterprise Personal Information Protection Evaluation Standard [J]. Information Network Security, 2014(4): 98.
[16] National Information Security Standardization Technical Committee. GB/T35273-2017, Information Security Technology—Personal Information Security Specification [EB/OL]. [2018-10-08]. http://c.gb688.cn/bzgk/gb/showGb?type=online&hcno=4FFAA51
[17] Li Xiaolin, Huang Chunlin. Challenges and Countermeasures for Chinese Enterprises in the Network Economy Era [J]. China Management Informationization, 2009, 12(17): 98-100.

Author Contributions

Xu Jicang: Research design, index design, index evaluation;
An Xiaomi: Methodology guidance;
Sun Jiarui: Literature review writing;

Wu Guojiao: Data collection;
Wang Li: Feedback revision and proofreading.

Note: Figure translations are in progress. See original paper for figures.