Recommendations for the Practice of Personal Information Protection Impact Assessment in China

Linlin Zhou[a], Yufei Wu[b], Haijun Wang[*], Yingyi Yao[c], Yu Wang[d], Zongshuang Jiao[e]

CATARC Intelligent and connected technology Co., Ltd., Tianjin, 300100, China

[a]zhoulinlin@catarc.ac.cn, [b]wuyufei@catarc.ac.cn
[*]wanghaijun2019@catarc.ac.cn, [c]yaoyingyi@catarc.ac.cn
[d]wangyu@catarc.ac.cn, [e]jiaozongshuang@catarc.ac.cn

Abstract. Personal information protection impact assessment, as a pre-risk management method, plays a crucial role in the personal information protection system, helping to accurately identify risk points, formulate targeted protection strategies, and thus improve the overall level of personal information protection. Due to the absence of corresponding procedural laws in China, enterprises still have some difficulties when conducting impact assessments. This analyzes the challenges in the implementation of impact assessment domestically, and propose an implementation plan for the impact assessment activities in light of the regulatory situation in China, which will facilitate the implementation of the impact assessment activities on the ground.

Keywords: Personal information protection impact assessment, PIA, DPIA, implementation practice, future prospect

1 Introduction

In the digital age, the illegal acquisition, sale, and abuse of personal information are common occurrences, posing a serious threat to individual rights and making the protection of personal information particularly urgent. In this context, Personal Information Protection Impact Assessment (abbreviated as "Impact Assessment.") has emerged. Impact Assessment is a proactive risk management method. It comprehensively assessing the risks that personal information processing activities may pose to individual rights and proposing corresponding risk control measures in order to keep risks within acceptable limits. In personal information processing activities, individuals are in a weak position relative to personal information processors, and once the adverse effects of personal information processing activities have been actualized, the harmful consequences are difficult to eliminate, so that prevention beforehand is far superior to relief afterwards in this process.

From a global perspective, China's personal information protection system still has some deficiencies and needs to be improved. The objective of this document is to propose an implementation framework for impact assessment, aiming to facilitate companies in effectively executing such assessments.

K. Zhang et al. (eds.), *Proceedings of the 4th International Conference on Management Science and Software Engineering (ICMSSE 2024)*, Advances in Engineering Research 244,
https://doi.org/10.2991/978-94-6463-552-2_9

2 Overview of Impact Assessment Supervision in Domestic and International Contexts

There are relevant requirements for impact assessments both domestically and internationally. For example, there are "Personal Information Security Impact Assessment" and "Personal Information Protection Impact Assessment" in china , while overseas there are "Privacy Impact Assessment(PIA)" and "Data Protection Impact Assessment(DPIA)".For example, domestically, there are 'Personal Information Security Impact Assessments' and 'Personal Information Protection Impact Assessments,' while internationally, there are 'Privacy Impact Assessments' and 'Data Protection Impact Assessments.' Although they are named differently and have slightly different focuses, their core meanings are similar.These assessments aim to analyze in advance the potential risks of personal information processing to personal rights and interests, and take measures to mitigate or avoid adverse effects and ensure the security and compliance of personal information processing[1].

2.1 Domestic Impact Assessment Supervision Situation

The recommended national standard GB/T 35273 "Information security echnology-Personal information security specification" was published in 2017 and updated in 20020. It clarifies the definition of Personal Information Security Impact Assessment: for personal information processing activities, test their legality and compliance, determine the various risks of damage to the legitimate rights and interests of personal information subjects, and evaluate various measures used to protect personal information subjects effectiveness process. What's more, GBT 35273 also puts forward specific requirements in terms of assessment content and assessment scenarios.

2021, the "Personal Information Protection Law of the People's Republic of China" was promulgated and implemented. The Articles 55 and 56 set forth requirements for personal information protection impact assessment, which means that impact assessment has changed from a recommended, optional requirement to a statutory, mandatory obligation.

The "Personal Information Protection Law of the People's Republic of China" and other regulations do not elaborate on the methods of impact assessment. There is a prominent problem in China's impact assessment system, that is, compared with the substantive law rules, its supporting procedural law rules are very inadequate, which will weaken the implementation and practice of the impact assessment system in China[2]. But fortunately, this research suggests that the recommended national standard GB/T 39335"Information security technology-Guidance for personal information security impact assessment" can serve as a fulcrum for its effective implementation . GBT 39335 clearly points out the basic principles, implementation process, and assessment details of the personal information security impact assessment. It is more focused on specific operations, and plays an important guiding role in the implementation of impact assessment.

2.2 Impact Assessment Supervision Situation Abroad

In the field of impact assessment research, some countries and regions have earlier exploration and practice than China. The "E-Government Act of 2002" issued by the United States in 2002 has regulated Privacy Impact Assessment(PIA) from three aspects: the responsibilities of the institution, the content of PIA, and the responsibilities of the head of the institution[3].To further guide the effective implementation of PIA, the relevant authorities have also released "Privacy Impact Assessment(PIA)Guide". Canada's PIA policy is also relatively well-developed, with the release of "Privacy impact assessment policy" in 2002, followed by the release of " Directive on privacy impact assessment""Interim policy on privacy protection" and other documents to gradually improve the management mechanism of impact assessment[4]. The New Zealand government issued "Privacy Impact Assessment Guidelines for Information Matching" in 1999, which specifically addresses the requirements of the information matching program, and in 2002, the Privacy Protection Authority further issued t"Privacy Impact Assessment Manual" to provide detailed guidance on privacy protection[5]. Considerable activity has been evident in the U.K. during 2008, following the publication of a PIA Handbook by the Information Commissioner's Office (ICO, 2007b). An overview of the project that gave rise to it appeared in CLSR 24, 3[6].

In 2017, the international standard ISO/IEC 29134 "information technology — Security techniques — Guidelines for privacy impact assessment" was published, describing the process of PIA process and the content of a PIA report. Its one of the most representative standards on PIAs, which was updated in 2023. The European Union adopted the General Data Protection Regulation (GDPR) in 2016.The GDPR's jurisdictional scope is extremely broad. It not only applies to the processing of personal data by data controllers and data processors established in the EU, but also applies to any business located outside the EU whose goods or services are targeted at individuals in the EU[7].Articles 35 and 36 of the GDPR provide for the application of the DPIA to data protection impact assessments (DPIA), and specify the content of the assessment. circumstances and specifies the content of the assessment.

3 Difficulties in the Implementation of Impact Assessment

Despite the clear definition of impact assessment requirements in "Personal Information Protection Law of the People's Republic of China", the procedural law rules supporting impact assessment are significantly flawed, resulting in challenges when implementing impact assessments. This chapter summarizes and analyzes these problems based on the current situation of enterprises' implementation of impact assessment.

3.1 The Inaccuracy in Grasping the Triggering Scenarios

The article 55 of "Personal Information Protection Law of the People's Republic of China" defines five situations in which impact assessment is required before data processing: (1) processing sensitive personal information;(2) using personal information

to conduct automated decision making;(3) entrusting, providing personal information processing to another party, or publicizing personal information;(4) providing personal information for any party outside the territory of the People's Republic of China; or(5) conducting other personal information processing activities which may have significant impacts on individuals. Among the five situations, the last clause reserves enough space and flexibility to deal with random and unforeseen problems[8].However, it also sets up difficulties in the process of carrying out the actual assessment by enterprises, as they often find it difficult to identify which activities pose a high risk to personal rights and interests because of the lack of a quantifiable and referable standard. This leads to the fact that enterprises will not be too accurate in grasping the trigger scenarios.

3.2 The Lack of Criteria for Judging Compliance

The article 56 of "Personal Information Protection Law of the People's Republic of China" sets out requirements for the content of impact assessments, includes:(1) whether the purposes and means of personal information processing are legitimate, justified and necessary;(2) the impact on individuals' rights and interests, and security risks; and(3) whether the protection measures taken are legitimate, effective, and compatible with the degree of risks. The first clauses refers to legitimate, justified and necessary, which can be considered as compliance personal information processing activities. However, the relevant regulations do not give criteria, or a list, for judging whether compliance is met or not. This makes it difficult for companies to simply determine the compliance of personal information processing activities.

3.3 The Lack of Understanding in Security Risk Rating Methods

In accordance with article 56 of "Personal Information Protection Law of the People's Republic of China", enterprises are mandated to conduct a comprehensive assessment of security risks arising from personal information processing activities. Although some enterprises try to identify security risks, the methods used are often varied and lack uniform standards and scientific basis, that potentially resulting in inaccurate evaluations and exposing them to compliance, legal, and economic risk.

4 Suggestions for Domestic Impact Assessment Implementation

In order to help enterprises solve the problems encountered in the implementation of impact assessment, this study clarifies the implementation process and methodology with reference to industry practice and GB/T 39335-2020. Upon analysis, Impact assessment can be implemented in the following five steps: trigger assessment judgment, determination of compliance with processing activities, data mapping analysis, analysis of security risk, risk disposal and continuous improvement.

4.1 Trigger Assessment Judgment

In the trigger assessment judgment stage, personal information processing scenarios need to be rigorously scrutinized to determine whether an impact assessment is required. This study proposes the following recommendations for the triggering of impact assessment: if a personal information processor recognizes that a personal information processing activity belongs to the first four scenarios of Article 56 of "Personal Information Protection Law of the People's Republic of China", he must conduct an impact assessment. Otherwise, the personal information processors can use the high-risk scenarios in 0. as a reference for deciding whether to do an impact assessment.

Table 1. Examples of high-risk individual processing activities.

No.	High-risk individual processing activities
1	Data processing involves the evaluation or rating of personal data subjects, in particular the assessment or prediction of the personal data subject's work performance, financial situation, health, preferences;
2	Use of personal information for automated analysis to give decisions that have a significant impact on person;
3	Match and merge data sets from different processing activities and apply them to the business;
4	Data processing involving vulnerable groups, such as minors, the sick, the elderly, low-income people, etc;
5	Application of innovative technologies or solutions such as biometrics, IoT, AI, etc;
6	The processing of personal information may result in the subject of the personal information not being able to exercise his or her rights, use services or receive contractual guarantees, etc.
7	The amount and proportion of sensitive personal information collected is high, and the frequency of collection is required to be high, which is closely related to personal experience, ideological views, health and financial status; Data are processed on a large scale, e.g., involving more than 1 million people, representing more than 50 per cent of a particular group, and covering a wide or concentrated geographical area;

4.2 Determination of Compliance with Processing Activities

Legitimate, justified and necessary can be collectively referred to as compliance, which can be the foundational principle. If processing activities are not compliant, they should be prohibited, regardless of whether they will pose a high security risk. Considering that there are no official standards for judging compliance, this study combines industry practices to propose standards for judging compliance to facilitate enterprises' judgment., as shown in 0. Only when the personal information processing activities meet the legality, legitimacy and necessity, can the next assessment work be carried out.

Table 2. Criteria for judging compliance.

Dimensions	Requirements	Notes
Legitimate	1) Not expressly prohibited by laws and regulations; 2) Relevant departments such as the national network information department, public security department, and security department did not declare that the processing activitis could not be carried out.	Only if two requirements are met at the same time can it be judged as legitimate
justified	1) The organization has planned to carry out the work related to the authorization and consent of the personal data subject (except where the consent of the personal data subject is not required); 2) Not contrary to the provisions of the relevant competent authority	Only if two requirements are met at the same time can it be judged as justified
necessary	1) Necessary for the performance of contractual obligations; 2) necessary to conduct business within the company; 3) Necessary for the fulfillment of the relevant requests made by our governmental departments.	As long as one of the requirements is met, it will be determined as necessary

4.3 Data Mapping Analysis

In the data mapping analysis stage, the personal information processor needs to provide a comprehensive description of the subject and form a data mapping table, in order to provide support for follow-up work.

4.4 Analysis of Security Risk

In the stage of comprehensive security risk analysis, the personal information processor should consider both the likelihood of security events and the degree of impact on personal rights and interests, and conduct a comprehensive analysis to determine the security risk level of personal information process activities.

Personal information processor can analyze the likelihood of security events from four aspects: (1) network environment and technical measures, (2) personal information processing process, (3) involved personnel and third parties, (4) business characteristics scale and security posture. The likelihood of security events can be categorized into levels 1, 2, 3 and 4. The higher the value of the level, the greater the likelihood of a security incident.

The impact of personal information processing activities on individuals can be analyzed from four dimensions: (1) limiting the right to make autonomous decisions, (2) triggering differential treatment, (3) damage to personal reputation or mental stress, (4) and damage to personal property. The degree of the impact can be categorized into levels 1, 2, 3 and 4. The higher the value of the level, the greater the likelihood of a security incident.

Personal information processor can preliminarily calculate the security risk as follow Equation 1, and get the security risk matrix as 0. The maximum value is then taken according to Equation 2. Finally, the security risk level can be obtained according to 0.

$$f(a_i, b_j) = a_i * b_j \tag{1}$$

$$y = \max(f(a_i, b_j)) \tag{2}$$

$$i = (1, 2, 3, 4),\ j = (1, 2, 3, 4),\ a_i = (1, 2, 3, 4),\ b_j = (1, 2, 3, 4)$$

a_i represents the likelihood of a security incident in the i dimension;

b_j represents the degree of the impact of the j dimension;

$f(a_i, b_i)$ represents the security risks associated with i and j;

y represents the maximum value of $f(a_i, b_i)$.

Table 3. The security risk matrix.

the security risks associated with i and j		network environment and technical measures	personal information processing process	involved personnel and third parties	business characteristics scale and security posture
		a_1	a_2	a_3	a_4
limiting the right to make autonomous decisions	b_1	$f(a_1, b_1)$	$f(a_2, b_1)$	……	……
triggering differential treatment	b_2	$f(a_1, b_2)$	……	$f(a_i, b_i)$	
damage to personal reputation or mental stress	b_3	……			
damage to personal property	b_4	……			

Table 4. Security risk reference table.

y	Levels of security risk
1-2	low security risk
3-6	medium security risk
8-9	high security risk
12-16	severe security risk

4.5 Risk Disposal and Continuous Improvement

In the risk disposal and continuous improvement stage, measures shall be taken for the processing activities with high security risk and severe security risk, so as to ensure that the risk is always controlled within an acceptable range.

5 Conclusion and Prospect

5.1 Conclusion

Personal information protection impact assessment plays a crucial role in safeguarding individual rights and interests. While some laws, regulations, and national standards in our country have stipulated requirements for impact assessments, the lack of corresponding procedural laws poses challenges to enterprise implementation. Drawing on industry experience and national standards, this paper proposes an implementation process for conducting impact assessments, which involves: trigger assessment judgment, determination of compliance with processing activities, data mapping analysis, comprehensive analysis of security risk, risk disposal and continuous improvement. Notably, in the trigger assessment judgment stage, this research supplements the example of high-risk individual processing activities to help companies identify high-risk activities. In judging the compliance of processing activities stage, criteria for judging compliance is proposed. In the stage of comprehensive security risk analysis, this study elaborates the impact assesment methods, solveing the doubts of enterprises. Overall, this research will facilitate the implementation of impact assessment in china.

5.2 Prospect

Furthermore, foreign research on impact assessment started earlier and the system is relatively mature. Therefore, we can learn the excellent experience of foreign countries to develop the impact assessment system in China.

In "Guidelines on Data Protection Impact Assessment (DPIA)" issued by the EU Data Protection Commission in 2017, WP29 also stated that it encourages the development of industry-specific DPIA frameworks to better address issues that arise in specific economic sectors or when using specific technologies or performing specific types of processing operations. The relevant authorities in China also can lead the industry by drawing on industry-specific knowledge and considering the characteristics of specific scenarios to formulate differentiated assessment plans to ensure the accuracy and effectiveness of the assessment, so as to better protect the security of personal information.

The UK's Information commissioner's Office (ICO) has published a unified DPIA template, which can simplify the process to enhance efficiency in the preparation of impact assessment reports.. It is recommended that the relevant departments learn from the ICO to issue a unified template for impact assessment reports to provide a clear and uniform yardstick for the fair and objective evaluation of corporate information protection.

References

1. Xin Ge.Personal Information Protection Impact Assessment System and Practical Guidelines[J].Confidentiality,2023,(06):57-59.DOI:10.19407/j.cnki.cn11-2785/d.2023.06.014.
2. Xinyi Dong, Xinyue Yuan.Procedural Regulation of Personal Information Protection Impact Assessment[J]. Journal of Jianghan University (Social Science Edition),2023,40(01):14-28+125.DOI:10.16387/j.cnki.42-1867/c.2023.01.002.
3. Yikai Liang,Mei Chen.The U.S. Privacy Impact Assessment System and Its Implications[J]. Intelligence Information Work,2022,43(05):60-70.
4. Yikai Liang, Mei Chen. Canadian privacy impact assessment policy: history, content, analysis, and implications[J]. Library and Intelligence Work,2021,65(17):142-151.DOI:10.13266/j.issn.0252-3116.2021.17.014.
5. Wright D. Making privacy impact assessment more effective[J]. The Information Society, 2013, 29(5): 307-315.
6. Warren A, Bayley R, Bennett C, Charlesworth A, Clarke R, Oppenheim C. Privacy impact assessments: international experience as a basis for UK guidance. Computer Law & Security Report April–June 2008;24(3):233–42.
7. Yuyang Gao. Study on the Extraterritorial Application of the "General Data Protection Regulation" [D]. Zhongnan University of Economics and Law,2023.
8. Xiangzhen Yao. Implementing Personal Information Protection Impact Assessment to Promote "Forward Movement" of Personal Information Protection[J]. China Information Security,2023,(03):73-75.