ChinaRxiv

AI translation · View original & related papers at
chinarxiv.org/items/chinaxiv-202304.00320

Data Protection Impact Assessment System: EU Legislation and China's Solution (Postprint)

Authors: Cui Congcong, Zhixin Xu

Date: 2023-04-01T16:15:50+00:00

Abstract

[Purpose/Significance] The Data Protection Impact Assessment (DPIA) regime introduced by the EU General Data Protection Regulation (GDPR) imposes new requirements on data controllers. By analyzing the relevant provisions of the DPIA regime in the GDPR and examining its legislative approach and core concepts, valuable insights can be provided for legislative efforts in China. [Method/Process] Through reviewing and systematically organizing legal instruments in the field of EU data protection, with the GDPR as a representative example, this study summarizes the background and evolution of the DPIA regime, and conducts an in-depth analysis of its main components, including the data protection model, applicable circumstances, basic procedures, and implementation process. [Results/Conclusion] The DPIA regime is capable of addressing increasingly complex and dynamic data security risk environments, holding significant practical value and reference significance. China's Personal Information Protection Law should establish a DPIA regime, with specific content encompassing the regulatory scope of DPIA, applicable circumstances, and the prior consultation obligations of data controllers, and should propose a data risk assessment model.

Full Text

Data Protection Impact Assessment System: EU Legislation and China's Approach

Cui Congcong, Xu Zhixin Internet Governance and Law Research Center, Beijing University of Posts and Telecommunications, Beijing 100876

Abstract: [Purpose/Significance] The Data Protection Impact Assessment (DPIA) system introduced by the EU General Data Protection Regulation (GDPR) imposes new requirements on data controllers. By analyzing the relevant provisions of DPIA in the GDPR and studying its legislative 思路

and core concepts, we can provide references for China's legislative work. [Method/Process] This paper reviews and organizes legal documents in the field of EU data protection represented by the GDPR, summarizes the background and evolution of the DPIA system, and deeply analyzes its main contents including the data protection model, applicable situations, basic procedures, and implementation processes. [Result/Conclusion] The DPIA system can address the increasingly complex and variable data security risk environment and has important practical value and reference significance. China's Personal Information Protection Law should establish a DPIA system, including regulatory objects, applicable situations, and prior consultation obligations of data controllers, and propose a data risk assessment model.

Keywords: Data Protection Impact Assessment; Risk-based Approach; Data Risk Assessment Model; Personal Information Protection Law **Classification Number:** G250 **DOI:** 10.13266/j.issn.0252-3116.2020.05.005

With the emergence of new technologies and applications such as cloud computing, big data, the Internet of Things, and artificial intelligence, automated processing of personal data has become ubiquitous, posing unprecedented threats to individual rights and freedoms in the digital age. In January 2012, the European Commission launched the reform process for EU personal data protection legislation, proposing the General Data Protection Regulation (GDPR) to replace the existing Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as the "95 Directive"). The GDPR officially entered into force on May 25, 2018, with the role of harmonizing EU approaches to help data controllers comply with relevant GDPR provisions and demonstrate that they have taken appropriate measures to comply with EU data protection regulations. As a core component of the EU data protection framework, the DPIA system has attracted widespread attention from enterprises and regulatory agencies worldwide, providing an ideal legislative reference for countries to address increasingly serious data security risk issues.

Currently, only a few scholars in the EU academic community, such as R. Gellert and F. Bieker, have conducted preliminary analyses of the DPIA system's concepts and practices, focusing primarily on changes in data risk concepts during the transition from Privacy Impact Assessment (PIA) to DPIA, as well as enterprise compliance methods based on GDPR text content. Beyond this, there are no more in-depth and systematic research results. Domestic research in China mostly remains at a superficial level of introducing the DPIA system, advocating for a shift in thinking regarding data processing behavior regulation, and proposing limited adjustments to domestic laws and regulations. No scholars have yet addressed how China's personal information protection legislation should learn from the DPIA system. This paper analyzes the relevant provisions of the data protection impact assessment system in the EU GDPR, studies the evolution process and core concepts of the DPIA system, proposes institutional designs for China's DPIA, and constructs a data protection system based on

a risk management approach, hoping to provide references for China's ongoing personal information protection legislation.

2. Background and Evolution of the EU DPIA System

2.1 Background of GDPR's Establishment of the DPIA System

Article 35(1) of the GDPR stipulates the general requirements for DPIA: data controllers should, before processing personal data, comprehensively consider the nature, scope, context, and purpose of the processing behavior, and assess the potential impact on personal data protection, particularly when using new technologies that may pose high risks to the rights and freedoms of natural persons. Before the GDPR was introduced, the EU already had requirements for data protection impact assessments for specific technology applications: first, the Privacy Impact Assessment and Data Protection Impact Assessment Framework (DPIAF) for RFID application fields; second, the DPIA template for smart grid and smart metering systems proposed by the European Commission's Smart Grid Working Group. These two documents were evaluated and revised by the EU WP29 Working Group. The basic points of the data protection assessment documents issued by the EU in the early stage all referred to the relevant content of the 95 Directive, but the actual implementation of impact assessments varied due to differences in the content of relevant documents.

Technology assessments and environmental impact assessments are forerunners in the field of impact assessment. The data protection impact assessment system introduced by the GDPR is a newcomer to this field. On the one hand, it does not directly copy relevant impact assessment systems; on the other hand, it is considered to have many similarities with PIA, which gradually developed since the 1990s and is widely applied mainly in Anglo-Saxon countries. Relevant viewpoints and literature on PIA, as well as guidance documents issued by Data Protection Authorities (DPAs), have had potential influences on the construction of the EU DPIA system.

2.2 From PIA to DPIA

The DPIA system is built upon the foundation of the PIA system, representing a product of adaptation and inheritance from the latter. The PIA system is defined as a method for analyzing and determining the impact of personal information processing projects, policies, plans, services, products, or other activities on privacy, requiring consultation and cooperation with stakeholders and the adoption of necessary remedial measures to avoid or reduce negative impacts. As the earliest European country to implement the PIA system, the UK published a PIA Code of Practice in 2007 by the Information Commissioner's Office (ICO) to refine and supplement relevant provisions of Article 51 of the UK's Data Protection Act, establishing a multi-stage PIA standard implementation process to assess and reduce privacy risks in the lifecycle of personal information processing projects. The French National Commission on Informatics and Liberties

(CNIL) issued a PIA protection framework in 2015, focusing on establishing a risk prevention and control system centered on technical and organizational means.

The PIA system established within the EU scope played a certain normative role in privacy protection. However, as it emerged before the formal establishment of DPIA legal obligations, it never became a mandatory legal obligation and could largely only serve a suggestive and guiding role. Additionally, PIA systems established by EU countries, including documents issued by the UK and France, generally adopted a checklist approach. Although enumeration can clearly indicate assessment content and reduce the implementation difficulty for organizations conducting PIA, it causes organizations to over-focus on fixed risks that have been listed, neither adapting to the dynamic changes in the risk environment nor addressing the specific risks and requirements of different data processing behaviors.

Compared with the previous PIA system, the DPIA system established by the EU GDPR can harmonize the consistency of data protection laws among member states. It has not only become a mandatory obligation under the EU's unified data protection legal framework but also possesses strong scalability and dynamic adjustment capabilities. However, the DPIA system's regulatory scope is limited to the field of data protection and does not address the privacy protection issues that the PIA system focuses on. Overall, by drawing on the establishment 思路 and implementation experience of the PIA system, the DPIA system possesses stronger operability, serving both as a compliance tool and a legal obligation, ensuring continuous security of data processing activities while guaranteeing that data controllers' and processors' data processing activities are reasonable and lawful.

3. Theoretical Foundation and Main Content of the EU DPIA System

3.1 Risk-Based Data Protection Model

3.1.1 Risk Composition in Data Protection The reasonable determination of risk is a prerequisite for correctly establishing the DPIA system. Risk analysis is usually presented as objective and neutral, but not entirely so. Some scholars believe that any risk-related decision involves two distinct but inseparable factors: objective facts and subjective viewpoints. Research on risk in both social governance and science and technology fields shows that risk-based practices are always closely related to their social environment and social values. Nevertheless, risks in data protection still require unified abstract concepts such as methodologies, templates, and processes that can be specifically implemented.

The risk handling methods stipulated by the GDPR reflect the dual dimensions of risk: risk assessment and risk management. Risk assessment measures the

objective risk level, focusing on the analysis of likelihood and severity, and its process can be divided into risk criteria, risk identification, and risk assessment steps. Risk management focuses on deciding whether to assume risk, and its decisions are usually accompanied by measures aimed at reducing risk levels.

To better map and understand the concept of risk in the GDPR, it is necessary to analyze the composition of risk itself. The EU WP29 Working Group defines risk as "the anticipation of an event and its consequences, estimated according to severity and likelihood." Specifically, the composition of risk in data protection should include three elements: Event: the occurrence or change of a specific situation. It may or may not happen and will produce some positive or negative consequences. Consequence: the result of an event. When the impact is negative, it can be called harm; when positive, it can be called benefit. Risk factors: individual or combined elements have inherent potential to cause harm. These determine whether and how risk occurs and determine the severity of the risk.

3.1.2 Shift in Data Protection Model to Risk Management In the era of big data, the personal information protection law based on the "informed consent principle" has gradually become formalistic, not only imposing heavy burdens on users and organizations but also failing to truly grant users actual data control rights. Therefore, the DPIA system introduced by the GDPR can be seen as an important measure to shift the regulatory and legislative path of data protection from "informed consent" to a "risk-based approach."

The EU DPIA system shifts its focus from unified regulation of data processing behaviors to dynamic risk management for specific data processing behaviors, running through project planning and execution processes to discover, assess, and address significant risks to data protection, personal rights, and freedoms as early as possible. Due to the universality and instantaneous nature of data processing behaviors, information transmission often has extensive and uncontrollable characteristics. Once risk hazards occur, they may cause irreparable damage to individuals and organizations. Therefore, the best solution for protecting data should focus on prevention and control measures before damage occurs rather than post-event remedies. The EU DPIA system re-establishes and expands the traditional data protection model, focusing on pre-emptive prevention methods, emphasizing the introduction and application of concepts such as "risk analysis," "impact assessment," and "lifecycle management," and promoting the transformation of traditional data protection regulatory models to a new data protection model based on risk management.

3.2 Basic Content of the EU DPIA System

3.2.1 Applicable Situations for the DPIA System The scope of the GDPR includes all fully or partially automated personal data processing behaviors within the jurisdiction of EU law, as well as non-automated personal data processing behaviors that create or are intended to create data profiles.

Although each relevant organization regulated by the GDPR will have a considerable number of data processing activities, the mandatory obligation of DPIA does not apply to every data processing behavior of an organization, otherwise the DPIA system would not be operable or economical in practice. Overall, unless the relevant data processing behavior meets the exemption conditions stipulated by the GDPR, DPIA methods must be implemented for any data processing behavior that "is likely to result in a high risk to the rights and freedoms of natural persons."

When a data processing behavior does not pose a possibility of high risk, the relevant organization will not need to fulfill the DPIA obligation. In addition, when the nature, scope, context, and purpose of a data processing behavior are very similar to an existing DPIA, the results of the existing DPIA can be used for similar processing without implementing a new DPIA method. Alternatively, when the processing behavior is specifically authorized by law, and that law has already implemented a corresponding DPIA at the time of its establishment, there is no need to implement a DPIA method again. Or when the data processing behavior meets the positive list requirements stipulated by the competent authority, the processing behavior does not need to implement a DPIA method, but must still strictly carry out processing activities according to the scope of behavior and relevant conditions required by the positive list.

In addition to establishing a positive list exempting DPIA obligations, the GDPR also requires regulatory authorities to formulate a negative list for data protection impact assessments, thereby clarifying in a checklist manner the data processing behaviors that must or need not undergo DPIA. For data processing behaviors with mandatory obligations, the GDPR specifically requires that when a new data processing technology is introduced, relevant organizations should proactively conduct data protection impact assessments. Additionally, when one of the following three situations exists, relevant organizations should conduct data protection impact assessments: Systematic and extensive evaluation of natural persons' personal situations based on automated decision-making systems and data profiling, where the evaluation results can affect the rights or obligations of natural persons; Processing activities of special categories of personal data or data related to criminal convictions and offenses; Large-scale systematic monitoring activities in public areas.

From the text, the specific applicable situations for DPIA stipulated by the GDPR are relatively vague and limited, but simultaneously reserve certain discretionary power for relevant EU regulatory authorities. The actual scope of DPIA obligations in practical work still needs to be determined based on legal texts combined with specific business practices.

3.2.2 Basic Process of the DPIA System For organizations conducting data processing activities, to achieve compliance under the EU GDPR framework and avoid huge fines and other serious consequences for violating DPIA mandatory obligations, they should proactively implement the basic process of

DPIA in their data business activities, mainly including four steps: Judgment on whether high risk may be caused; Judgment on whether exceptional circumstances apply; Implementation of the DPIA method; Judgment on whether the remaining risk is still high. Subsequently, the organization will decide whether to conduct prior consultation with the regulatory authority based on the actual risk level, as shown in Figure 1 [Figure 1: see original paper].

(1) **Judgment on whether high risk may be caused.** As a data controller, the organization should fully consider the nature, scope, context, and purpose of the data processing behavior, and assess in advance the high risk that the expected behavior may pose to the rights and freedoms of natural persons. If the organization determines that the risk level is indeed low, there is no need to continue implementing the subsequent processes of the DPIA system.

(2) **Judgment on whether exceptional circumstances apply.** The data controller should determine whether it can be exempted from implementing DPIA according to the exemption conditions stipulated by the GDPR: one is when the regulatory authority enumerates data processing behaviors that do not require DPIA according to Article 35(5) of the GDPR; the other is data processing behaviors with specific legal basis as stipulated in Article 35(10) of the GDPR. If the organization determines that its data processing behavior has very similar risk situations to existing DPIA methods, it can confirm the applicable method in this step.

(3) **Implementation of the DPIA method.** In the implementation process of the DPIA method, the data controller should seek the opinions and assistance of the Data Protection Officer (DPO) on the specific methods for conducting data protection impact assessments, and take into account codes of conduct formulated by EU member states, industry associations, and other institutions. Without prejudice to commercial interests, public interests, and the security of processing behaviors, the data controller should solicit opinions from data subjects or their representatives on the data processing behavior. The data controller should supervise the relevant data processing behavior to ensure the implementation of DPIA assessment results and risk response methods.

(4) **Judgment on whether the remaining risk is still high.** If the DPIA assessment results indicate that the relevant organization has not taken sufficient data protection measures to reduce the high risks generated during the data processing behavior, the data controller should conduct prior consultation with the regulatory authority before starting the data processing activity. If the regulatory authority believes that the processing activity to be carried out by the data controller or processor will violate the provisions of the GDPR, especially when the data controller cannot adequately identify or reduce risks, it should provide written recommendations to the data controller and data processor within 8 weeks of receiving the consultation request (which can be extended by another 6 weeks de-

pending on the complexity of the data processing activity).

3.2.3 Specific Implementation of the DPIA Method

(1) **Implementing entity.** The implementation of the DPIA method is the third step of the basic process and the core content of the DPIA system. The DPIA method should be implemented before the data processing behavior begins. The implementing entity can be the data controller, data processor, or DPO. The data controller is responsible for ensuring the implementation of DPIA, and the specific implementation can be completed by internal or external personnel of the organization, but the data controller is ultimately responsible for this legal obligation. If the data processing behavior is executed entirely or partially by the data processor, the data processor should assist the data controller in implementing DPIA and provide any necessary information. The data controller should seek the DPO's advice, and the DPO should supervise the implementation of DPIA. Information on the DPO's appointment, advice, and relevant decisions made by the data controller should be recorded in the DPIA documentation.

(2) **Minimum requirements.** The GDPR stipulates the minimum requirements for relevant organizations to implement the DPIA method: systematic description of the intended processing behavior and purposes, as well as the legitimate interests pursued by the controller; assessment of the necessity and appropriateness of the processing behavior related to the processing purposes; assessment of risks to the rights and freedoms of data subjects; intended risk prevention measures mainly include considering the rights and legitimate interests of data subjects and other relevant personnel, ensuring personal data security, and demonstrating protection measures, security means, and mechanisms that comply with GDPR requirements, which will be considered as intended risk prevention measures in the next DPIA method; to achieve the expected effects of DPIA, it is necessary to comprehensively document risk assessment results, produce standard reports, and have the data controller decide whether to make them fully or partially public (at least the conclusion part should be made public), demonstrating the transparency and accountability of data processing activities to facilitate evaluation and comparison by regulatory authorities, enterprises, and the public; after documentation and archiving, the GDPR requires the controller to supervise and review the data processing behavior (at least when the risks caused by the processing behavior change) to assess and confirm whether the processing behavior is carried out according to the DPIA assessment results (see Figure 2 [Figure 2: see original paper]).

(3) **Content scalability.** Above the minimum requirements, the content of the DPIA method is scalable. Different data controllers can flexibly determine the specific process of DPIA to adapt to their business prac-

tices, and even small and micro data controllers can design and implement DPIA methods suitable for their execution. However, regardless of the form, DPIA must reflect the assessment of real risks and allow data controllers or processors to take measures to address these issues. The EU WP29 Working Group encourages the joint development of DPIA standard frameworks within specific industries or fields, enabling DPIA to be applied to different types of data processing behaviors to solve differentiated problems. Additionally, the DPIA framework should also consider the connection with codes of conduct or industry standards. If a data controller's processing behavior complies with the relevant requirements of codes of conduct or industry standards, it can be used to prove that appropriate risk management measures have been implemented for the processing behavior, thus exempting it from repeatedly implementing similar DPIA methods.

(4) **Dynamic adjustment requirements.** Due to the rapid changes in the risk environment, it is crucial for data controllers to continuously implement the DPIA method throughout the entire lifecycle of data processing activities to maintain a stable level of data protection in a dynamic risk environment. Specifically, data controllers need to analyze new risks arising from changes in the nature, scope, context, and purpose of processing behaviors, and update DPIA accordingly. Data processing behaviors may pose potential high risks to the rights and freedoms of natural persons again due to changes in the risk environment, even when they have already implemented DPIA methods and achieved low-risk standards at that time. In such cases, relevant organizations need to iterate the DPIA method according to at least the minimum requirements. For example, an automated decision-making system may trigger the execution conditions of the DPIA method as it becomes socially risky with technological advancement; conversely, an automated decision-making system that adds human control factors, or monitoring activities that are no longer systematic, may show reduced risk levels in their risk assessment and no longer require DPIA implementation. The emergence or upgrading of new data processing technologies will continuously generate new types of risks. As a good practice, data controllers should continuously conduct data protection impact assessments and regularly re-evaluate them to ensure that risk management measures are consistent with the dynamic nature of the risk environment.

4. Implications of the EU DPIA System for Chinese Legislation

4.1 New Data Protection Model Under the EU DPIA System

The cybersecurity situation changes rapidly, and "static, uniform regulations that focus on security baselines" can no longer provide substantive security

guarantees for personal data. The concept of relative security shows that reducing risk to zero is unrealistic, so the main task of data protection is to identify risks and reduce the risk level of specific data processing behaviors to a level that data controllers can bear. The GDPR sets general obligations for data controllers through a "risk-based approach," emphasizing the construction of different risk governance rules based on the likelihood and severity of damage to natural persons' rights and freedoms from data processing behaviors, and requiring data controllers to incorporate them into internal decision-making. This shifts from a top-down government regulatory model to a self-executing model from within, which reduces institutional implementation costs while effectively improving data protection efficiency and effectiveness.

The new data protection model constructed by the EU DPIA system can be understood as two specific stages: risk assessment and risk management. Risk assessment methods can use facts and assumptions to evaluate the likelihood of potential harm to data subjects from data processing behaviors, matching the circumstances of data processing behaviors with enumerated potential harm factors, and using the degree of matching as one of the considerations for risk assessment. Assessment results can be divided into five levels: minor, small, moderate, high, and severe. After completing risk assessment, data controllers need to conduct risk management for identified potential harms. Risk management should be reflected in the decision-making process of data controllers, selecting appropriate preventive measures against short-term and long-term data protection risks in combination with technical capabilities and social context. Data risk management needs to design different data controller protection obligations according to different risk levels: under general risk and lower levels, data controllers' obligations can be appropriately reduced or partially exempted; while under high risk and severe risk levels, data controllers have higher data protection obligations and are obligated to reduce risks below the general risk level. If data controllers cannot control risks below the general risk level, or find it difficult to identify or assess their risk levels, they must not conduct corresponding data processing behaviors and should consult with regulatory authorities for relevant advice. It should be pointed out that even at lower risk levels, data controllers should fulfill minimum protection obligations to ensure that data subjects' rights and freedoms are protected in any risk environment.

The rapid development and widespread application of data processing technologies make traditional regulatory models difficult to address the complex and variable data protection issues in the big data era. The data protection model advocated by the EU DPIA system replaces the "all-or-nothing" judgment in traditional regulatory paths by quantifying risk levels, which can both improve the operability of data protection and reduce enterprise compliance pressure while promoting the rational use of data. Therefore, China's data protection model should also attempt to shift from the static "informed consent" traditional framework to a dynamic "risk-based approach" 思路, establishing a personal information protection legislative model under the new data security paradigm.

4.2 China's Personal Information Protection Law Should Establish a DPIA System

Currently, China's data protection legislation is scattered across the Cybersecurity Law, E-Commerce Law, Consumer Rights Protection Law, Criminal Law Amendment (VII), Criminal Law Amendment (IX), and the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection. The above legislation basically puts forward basic requirements for data controllers from the principles of legality, legitimacy, and necessity that data collection and utilization should follow, as well as security protection obligations such as confidentiality and breach notification, but does not mention the data protection impact assessment system. The national standard "Information Security Technology - Personal Information Security Impact Assessment Guidelines (Draft for Comments)" released on June 11, 2018 (not yet officially adopted) provides institutions and enterprises with the basic framework, methods, and processes for personal information security impact assessment for self-assessment use, while also providing guidance and basis for national competent authorities, third-party evaluation agencies, and others to carry out personal information security supervision, inspection, and evaluation. This standard is positioned as a recommended standard rather than a mandatory standard. Without mandatory requirements, there is no guarantee, and the lack of regulatory authorities and accountability mechanisms will directly affect the rights relief of data subjects, thereby indulging enterprises in selectively or substantively adopting DPIA system methods to win market trust. The adoption of this non-mandatory data protection model may even exacerbate the high risks to natural persons' rights and interests.

With the continuous development of information technology, China's personal data security will face greater risks. The DPIA system under the EU data protection framework has strong preventive capabilities, reducing personal and social data protection risks to sufficiently low levels. It also has strong dynamic and scalable procedures that can be adopted by a wide range of organizations. China's existing legislation includes environmental protection impact assessment and food safety risk assessment, which are similar risk prevention mechanisms to the DPIA system. From the implementation effects of the former, it is technically feasible for China to set the DPIA system as a mandatory obligation.

Through the implementation of DPIA obligations, on the one hand, it strengthens the responsibilities of data controllers, making them focus on enhancing data protection awareness and mechanism construction throughout the entire process of data processing behaviors, thereby winning market reputation and data subject trust. On the other hand, it can achieve a balance between security and efficiency in the big data era, govern the currently widespread data abuse behaviors, clearly require enterprise organizations to give consideration to the security baseline of data protection while using data to conduct business, and make DPIA obligations an important component of their upfront investment

and daily operations, reducing the risks and hazards brought by potential data harm incidents to enterprises while safeguarding personal rights and freedoms and social public security.

4.3 Conception of China's DPIA System

4.3.1 Regulatory Objects of DPIA The regulatory objects of DPIA include not only single data processing behaviors but also a group of similar high-risk data processing behaviors. Determining whether processing behaviors are similar requires considering whether the nature, scope, context, purpose, and risk level of the processing behaviors are consistent, mainly including: whether the processing behavior itself is similar, whether the data subjects are similar, and whether the products or environments relied upon by the processing behavior are similar. Generally, it is more reasonable and economical to treat a group of similar data processing behaviors as the regulatory object of DPIA, such as when public institutions plan to establish data sharing processing platforms, or when multiple controllers plan to introduce data sharing applications in a certain industry.

The purpose of establishing the DPIA system is to systematically study and judge new situations that may lead to high risks to natural persons' rights and freedoms. For cases that have already been studied—i.e., the same processing behavior conducted in a specific environment and for a specific purpose—there is no need to conduct a new DPIA. This includes situations where similar technology is used to collect the same type of data for the same purpose, and similar data processing behaviors that can be applied to multiple controllers. In these cases, regulatory authorities should organize the formulation of DPIA standard schemes for the same type of data processing behavior and make them public. Data controllers of similar behaviors should implement the measures described in the standard scheme. If an independent DPIA scheme needs to be used, justifiable reasons must be provided to the competent authority.

When data processing behaviors involve multiple controllers, they need to clearly divide their respective obligations in the DPIA, being responsible for different measures to reduce risks or protect data subjects' rights and freedoms. Additionally, DPIA can be used to assess the data protection risks of data processing technologies, products, or services. The same technology, product, or service may be used by different data controllers for different types of data processing behaviors. Data controllers deploying relevant products have the obligation to implement DPIA when conducting specific data processing but can also choose to use DPIA schemes provided by product suppliers that can be applied to corresponding data processing behaviors.

4.3.2 Applicable Situations for DPIA Not all data processing behaviors require DPIA implementation. DPIA must only be implemented when the processing behavior may pose high risks to natural persons' rights and freedoms. If data controllers are unclear whether DPIA needs to be implemented, especially

when introducing new data processing technologies or solutions, it is recommended that they implement DPIA, as DPIA is a compliance tool to help data controllers comply with data protection laws. To determine whether to implement DPIA, data controllers should consider the following data security risk behaviors:

(1) **Evaluation or assessment of data subjects.** Including analysis and prediction, especially using data about data subjects' work performance, economic status, health, personal preferences or interests, behavior, location, movement, etc.

(2) **Automated decision-making with legal effect or similar significant impact.** Such data processing behaviors may lead to exclusion or discrimination against individuals by specific entities.

(3) **Systematic monitoring.** Used to observe, monitor, or control data subjects' behavior, mainly including systematic collection of personal data through networks or systematic monitoring of public areas.

(4) **Processing of sensitive data.** Sensitive data refers to data that, once leaked or misused, can easily endanger personal or property safety or cause damage to personal dignity or discriminatory treatment, including ID numbers, communication content, accommodation information, communication records, etc. Processing sensitive data includes collecting, storing, analyzing, providing externally, and sharing sensitive data.

(5) **Large-scale data processing.** When determining whether a data processing behavior is large-scale, the following factors should be considered: the number of data subjects, including specific numbers or population proportions; data volume and data types; duration of data processing behavior; geographical scope of data processing behavior.

(6) **Matching or combining datasets.** The act of associating or merging two or more datasets collected for different purposes or belonging to different data controllers. This data processing method exceeds data subjects' reasonable expectations in general data processing behaviors.

(7) **Processing of data of vulnerable groups.** Due to the increased power imbalance between data subjects and data controllers, when processing such data, some data subjects may not be able to effectively refuse or object to data processing behaviors related to them. In such cases, DPIA needs to be implemented to reduce risks to data subjects. Vulnerable groups may include children, employees, patients, and other groups requiring special protection, as well as other situations where there is a power disparity between data subjects and data controllers.

(8) **Innovative applications or use of new technologies.** The use of new technologies usually triggers the execution conditions of DPIA, as using new technologies typically means new forms of data collection and use,

which may pose high risks to individuals' rights and freedoms. The application of new technologies will bring unknown consequences to individuals and society, and the DPIA system will help data controllers understand and address such risks.

(9) **Preventing data subjects from exercising rights, using services, or concluding contracts.** This includes automated decision-making behaviors made by institutions through data processing activities, such as banks automatically screening customers through credit data to decide whether to provide them with loans.

Data controllers can assess data protection risks by matching expected data processing behaviors with the above risk situations and using the degree of matching as a risk factor. In most cases, if data controllers believe their data processing behavior meets two of the above situations, they need to implement DPIA, unless the data controller has sufficient reasons and evidence to show that the behavior cannot pose high risks. In such cases, the data controller should explain the decision not to implement DPIA and record the reasons for not implementing DPIA and the opinions of the competent authority.

4.3.3 Data Risk Assessment Model The data protection assessment model is a method to ensure effective compliance with data protection obligations. This model can conduct risk management for specific data processing behaviors by implementing DPIA, assisting data controllers in selecting appropriate intended risk prevention measures to reduce risk levels. The data minimization principle is the necessity principle of the data protection assessment model, requiring that any processing behavior, whether overall or at each step, must not collect, process, or use more personal data than necessary to achieve the processing purpose. As an important factor in data protection-friendly design, the data minimization principle should be embedded into the technical design and configuration environment of network service providers and applied to actual data processing activities throughout the complete data lifecycle.

The data protection assessment model can be used to assess the risks to natural persons' rights and freedoms, identifying potential risk sources and damage consequences. Based on these factors, DPIA can classify data protection risks into different levels to distinguish different impact degrees and ensure fulfillment of corresponding data protection obligations.

(1) **Availability.** The processed personal data must be available and can be correctly used in the intended processing activities. Data subjects must be able to effectively access data, the data format should be recognizable, and data controllers should ensure that data is processed in the intended manner. Therefore, data availability includes the system's ability to find specific data, the system's ability to enable data subjects to access data, and the ability to effectively display data content.

(2) **Integrity.** The processed personal data must be ensured to be intact, com-

plete, and up-to-date. Data controllers should have the ability to identify or exclude data biases to locate or correct data attributes or content.

(3) **Confidentiality.** No one may access the processed personal data without authorization. "Anyone" here includes unauthorized third parties outside the data controller, employees of technical service providers, and personnel within the data controller who are unrelated to the corresponding processing behavior.

(4) **Non-linkability.** Data processing behaviors should only be used for the intended purpose at the time of data collection. In some situations, the processed personal data may be further used beyond the intended purpose and matched or combined with other publicly available datasets. These processing behaviors usually exceed reasonable processing purposes and are only legal under specific stipulated circumstances (e.g., for public interest purposes, for scientific or historical research purposes, for statistical purposes, and without infringing on data subjects' rights and freedoms). Non-linkability usually needs to be achieved through technology and solutions, using means such as data anonymization to isolate subsequent processing from previous processing, ensuring that data processed within the organization and information system are not interrelated.

(5) **Transparency.** As a prerequisite for implementing DPIA, sufficient transparency is required throughout the entire lifecycle from data generation to destruction. Only with transparency satisfied can data subjects express informed consent that meets legal requirements. In data processing activities, data controllers need to ensure that data subjects and regulatory authorities have the ability to identify risks and raise objections. Data subjects and regulatory authorities must fully understand relevant information about data processing behaviors: attributes of collected and processed data, information systems and configuration environments used to achieve intended processing purposes, and subjects responsible for data and system security in data processing behaviors.

(6) **Intervenability.** Data subjects should be effectively granted the rights to access, correct, delete, and object at any time, and data controllers have the obligation to implement corresponding rights protection measures. To this end, controllers must have the ability to intervene in data attributes, content, and status throughout the entire lifecycle of data processing activities.

4.3.4 Prior Consultation Obligation The prior consultation obligation arises after DPIA implementation when the remaining risk is still high. High remaining risk means that data subjects may encounter significant or irreversible consequences that cannot be resolved (e.g., illegal data access will cause life threats, layoffs, property dangers to data subjects), and when risks are obvious (e.g., failure to repair well-known vulnerabilities). As long as data controllers

cannot find sufficient measures to reduce risks to an acceptable level, they need to consult with regulatory authorities.

When the personal data stored by data controllers has used appropriate technologies and solutions (e.g., effective full-disk encryption, strong key management, appropriate access control, complete security backups) and can fully protect the relevant rights of data subjects, if data controllers determine that data protection risks have been sufficiently reduced, they can start data processing activities without consulting regulatory authorities. If data controllers cannot resolve identified risks (i.e., remaining risks are still high), they must consult with regulatory authorities in advance. Data controllers conducting data processing for public interest purposes should also consult with regulatory authorities in advance and obtain prior authorization. It should be pointed out that regardless of whether prior consultation with supervisory authorities is needed, the obligation to retain DPIA records and appropriately update DPIA remains.

When data controllers conduct prior consultation with regulatory authorities, they should provide the following information: the respective responsibilities of controllers, joint controllers, and processors in the data processing behavior; the intended purposes and means of processing data; measures to protect data subjects' rights and freedoms; contact information of the DPO; DPIA results, etc.

References

[1] The EU general data protection regulation is the most important change in data privacy regulation in 20 years [EB/OL]. [2019-04-23]. https://eugdpr.org/.

[2] Guidelines on data protection impact assessment and determining whether processing is "likely to result in a high risk" for the purposes of regulation 2016/679 [EB/OL]. [2019-04-04]. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_{id}=611236.

[3] GELLERT R. Understanding the notion of risk in the general data protection regulation [J]. Computer law & security review, 2018, 34(2): 279-288.

[4] BIEKER F, FRIEDEWALD M, HANSEN M, et al. A process for data protection impact assessment under the European general data protection regulation [C]// APF 2016. Lecture notes in computer science. Cham: Springer, 2016: 21-37.

[5] GAO Fuping. International rules for personal data protection and utilization: Origins and trends [M]. Beijing: Law Press, 2016.

[6] European Commission. Privacy and data protection impact assessment framework for RFID applications [EB/OL]. [2019-01-12]. https://danskprivacynet.files.wordpress.com/2008/06/2011-0068.pdf.

[7] European Commission. Recommendation of 10 October 2014 on the data protection impact assessment template for smart grid and smart

metering systems [EB/OL]. [2019-01-13]. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014H0724&from=EN.

[8] VAN D, GELLERT R, ROMMETVEIT K. A risk to a right? Beyond data protection risk assessments [J]. Computer law & security review, 2016, 32(2): 286-306.

[9] CLARKE R. Privacy impact assessment: its origins and development [J]. Computer law & security review, 2009, 25(2): 123-135.

[10] WRIGHT D, DE HERT P. Privacy impact assessment [M]. Dordrecht: Springer Netherlands, 2012.

[11] CNIL. Privacy risk assessment: methodology (how to carry out a PIA) [EB/OL]. [2019-02-01]. http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf.

[12] XIAO Dongmei, TAN Lige. The EU data protection impact assessment system and its implications [J]. Journal of Library Science in China, 2018, 44(5): 76-86.

[13] WRIGHT D. The state of the art in privacy impact assessment [J]. Computer law & security review, 2012, 28(1): 54-61.

[14] WRIGHT D, GELLERT G, GUTWIRTH S, et al. Precaution and privacy impact assessment as modest towards risk governance [M]. Luxembourg: European Commission, 2011.

[15] BERNSTEIN P L. Against the Gods: the remarkable story of risk [M]. New York: John Wiley & Sons, 1996.

[16] EWALD F. Insurance and risk [M]. Chicago: The University of Chicago Press, 1991.

[17] WYNNE B. Risk and environment as legitimatory discourse of technology: reflexivity inside-out [J]. Current sociology, 2002, 50(3): 459-477.

[18] POWER M. Organized uncertainty: designing a world of risk management [M]. Oxford: Oxford University Press, 2007.

[19] ISO. Risk management - Principles and guidelines [EB/OL]. [2019-02-17]. https://www.iso.org/standard/43170.html.

[20] WARNER F. Risk: analysis, perception and management - a report of a royal [M]. London: The Royal Society, 1992.

[21] CHENG Ying. Data protection impact assessment system under risk management mode [J]. Journal of Cyber and Information Security, 2018, 4(8): 63-70.

[22] Statement on the role of a risk based approach in data protection legal frameworks [EB/OL]. [2019-03-25]. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_{en}.pdf.

[23] HONG Yanqing. “Management-based regulation” - reconstruction of network operators’ security protection obligations [J]. Global Law Review, 2016, 38(4): 20-40.

[24] GELLERT R. Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative [J]. International data privacy law, 2015, 5(1): 3-19.

[25] PDPC. Guide to data protection impact assessment [EB/OL]. [2019-04-14]. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guide-to-dpias—011117.pdf.

[26] FAN Wei. Path reconstruction of personal information protection in the big data era [J]. Global Law Review, 2016, 38(5): 92-115.

[27] Standardization Administration of China. Information security technology - Personal information security impact assessment guidelines (draft for comments) [EB/OL]. [2019-03-28]. https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20180613180739930746&norm_

[28] BINNS R. Data protection impact assessments: a meta-regulatory approach [J]. International data privacy law, 2017, 7(1): 22-35.

[29] HU Wentao. Conception of defining personal sensitive information in China [J]. China Legal Science, 2018, 35(5): 235-254.

[30] BIEKER F, MARTIN N, FRIEDEWALD M, et al. Data protection impact assessment: a hands-on tour of the GDPR’s most practical tool [C]// IFIP. Advances in information and communication technology. Cham: Spring, 2018: 207-220.

Author Contributions: Cui Congcong: Responsible for topic selection, outline formulation, and paper revision; Xu Zhixin: Responsible for data collection and initial paper drafting.

Data Protection Impact Assessment: EU Legislation and China Plan

Cui Congcong, Xu Zhixin Institute of Internet Governance and Law, Beijing University of Posts and Telecommunications, Beijing 100876

Abstract: [Purpose/Significance] The Data Protection Impact Assessment (DPIA) introduced by the General Data Protection Regulation (GDPR) imposes new requirements on data controllers. By analyzing the relevant provisions of DPIA in the GDPR and studying its legislative ideas and core concepts, it could provide reference for relevant legislative work in China. [Method/Process] This paper reviews the legal documents in the field of EU data protection represented by the GDPR, summarizes the background and evolution of the DPIA system, and then deeply analyzes its data protection pattern, applicable situations, basic processes, and execution processes. [Result/Conclusion] The DPIA can cope with the increasingly complex and variable risk environment of data security, which has important practical value and reference significance. China’s personal information protection law should establish the DPIA system, which

includes DPIA's regulatory objects, applicable situations, and data controllers' prior consulting obligations, and propose a data risk assessment model.

Keywords: DPIA; risk-based approach; data risk assessment model; personal information protection law

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

Source: ChinaXiv — Machine translation. Verify with original.