A Study on the EU Data Protection Officer System: Postprint

Authors: Xiao Dongmei, Cheng Siwen

Date: 2023-07-26T00:00:00+00:00

Abstract

[Purpose/Significance] The Data Protection Officer (DPO) system in the EU's new data protection regulation (GDPR) has garnered significant attention. Tracing the evolutionary path of the DPO system, analyzing the establishment and specific responsibilities of DPOs, and examining the implementation and impact of the EU DPO system are not only crucial for Chinese enterprises' trade with Europe, but also serve as an important reference for the development of China's relevant regulatory framework.

[Methods/Process] By reviewing the GDPR provisions concerning DPOs and related procedural documents, it is found that data controllers/processors should appoint a Data Protection Officer under three circumstances stipulated by the GDPR. The responsibilities of DPOs include informing and advising relevant staff of data controllers, monitoring the compliance of data processing activities, acting as a contact point for data subjects, cooperating with supervisory authorities, recording and archiving data processing activities, training, and confidentiality, among others.

[Results/Conclusion] The establishment of DPOs has profound implications for ensuring compliance by data controllers and reducing the burden on supervisory authorities. The implications of the EU DPO system for Chinese enterprises/institutions lie in: DPOs should be appointed in accordance with GDPR provisions, and comprehensive data protection oversight procedures should be established; the implications for China's data protection supervision and mechanism construction include: clearly stipulating that data controllers should establish dedicated data protection positions and employ professionals, imposing corresponding accountability and penalties on non-compliant data controllers, and enhancing the capacity building of data protection authorities.

Full Text

Preamble

A Study of the EU Data Protection Officer System

Xiao Dongmei, Cheng Siwen
Law School of Xiangtan University, Xiangtan 411105

Abstract

[**Purpose/Significance**] The Data Protection Officer (DPO) system under the EU's new data protection regulation (GDPR) has attracted considerable attention. Tracing the evolutionary path of the DPO system, analyzing the establishment and specific responsibilities of DPOs, and examining the implementation and impact of the EU DPO system are not only relevant to Chinese enterprises trading with Europe but also serve as an important reference for constructing China's relevant regulatory framework. [**Method/Process**] By 梳理 ing the DPO-related provisions in the GDPR and related legislative texts, this study finds that data controllers/processors should appoint a DPO in three circumstances specified by the GDPR. The responsibilities of DPOs include informing and advising relevant staff of data controllers, monitoring compliance of data processing, liaising with data subjects, cooperating with supervisory authorities, maintaining records and documentation of processing activities, training, and confidentiality obligations. [**Result/Conclusion**] Establishing DPOs has far-reaching implications for ensuring data controller compliance and reducing the burden on supervisory authorities. The implications of the EU DPO system for Chinese enterprises/institutions are: DPOs should be appointed in accordance with GDPR provisions, and a complete data protection supervision process should be designed. For China's data protection supervision and mechanism construction, the 启示 include: clearly stipulating that data controllers should establish specialized data protection positions and professionals; imposing corresponding accountability and penalties for non-compliant data controllers; and strengthening the construction of data supervisory authorities.

Keywords: Data Protection Officer; Personal Data Protection; Compliance

Introduction

The rapid development of mobile internet and widespread adoption of various smart terminals have propelled human society into the era of big data and the Internet of Things. Big data collection, processing, and utilization activities have deeply penetrated every sphere of social life including healthcare, technology, education, sports, commerce, and economics, with a global data torrent rushing toward us. While big data can make the world more transparent—where more data means more precise understanding and prediction, and many previously intractable social problems can be solved—it also poses serious challenges to traditional national boundaries and national security [1]. The EU's 2016 General

Data Protection Regulation (GDPR) demonstrates the EU's stance on personal data protection in the big data era. The GDPR transformed previous data protection rules based on automated computer processing, establishing a stricter data protection framework urgently needed to respond to new data risks [2].

The establishment of Data Protection Officers (DPOs) is one of the important provisions in the GDPR. Through DPOs who supervise the compliance of internal data processing activities of data controllers (natural or legal persons, public authorities, agencies, or other bodies that alone or jointly determine the purposes and means of processing personal data) or processors (natural or legal persons, public authorities, agencies, or other bodies that process personal data on behalf of the controller), the GDPR strengthens data protection throughout the collection and processing chain. This provision occupies an important position in the EU data protection framework and has attracted considerable attention from relevant enterprises and practitioners, with numerous news reports and social media posts discussing DPOs. However, literature searches show that academic research on this topic remains scarce. In foreign academia, only a few scholars such as E. Lachaud [3] and R. Miguel [4] have conducted preliminary analyses of DPOs' legal status, obligations, and responsibilities, with no in-depth research findings discovered to date. Domestically, aside from mentions of the DPO system in relevant articles [5-6], no specialized academic papers on DPOs have been found. Although academic attention to the DPO system appears insufficient currently, its impact will become increasingly prominent following GDPR's formal implementation on May 25, 2018. Research on the operation of the DPO system and resolution of related theoretical issues will become increasingly important, concerning not only Chinese enterprises' trade with Europe but also helping advance the construction of a Chinese regulatory framework that balances data economy development with data protection.

2. The Origin of the EU DPO System

2.1 Early Development of DPOs in the EU

Early personal data was categorized under the right to privacy. As personal data collection and use increased dramatically, it created a massive impact on the traditional "private sphere." "Under the privacy framework, personal data lacked effective capacity to counter information abuse by public and private entities" [7], prompting most countries worldwide to focus on personal data protection. In the 1970s, European countries began personal data protection legislation and institutional construction, with Germany being the most typical example. Germany's 1977 Federal Data Protection Act first introduced the term DPO (expressed in German as "beauftragter für den datenschutz"), stipulating its role as ensuring data controllers' compliance with data protection provisions. In 2001, Germany amended its Federal Data Protection Act, explicitly providing that "public and private bodies shall support DPOs in exercising their duties" [8], gradually bringing DPOs into greater prominence. After entering the 21st century, the rise of social networks and cloud computing, alongside the formation

of black data industry chains, led to rampant data leaks and illegal data trading in Germany. In 2009, the German Federal Parliament amended the Act again, elevating DPOs' legal status and granting them additional powers.

Beyond Germany, other European countries' data protection legislation also contained DPOs or similar concepts, which can be divided into two types: mandatory DPOs and voluntary DPOs. Mandatory DPOs refer to positions that must be established by law under certain conditions, adopted by countries including Belgium, Spain, and Hungary. Belgium's Data Protection Act (1992) and subsequent decrees and amendments stipulated that organizations and groups collecting and processing citizens' personal data on a large scale should appoint DPOs to ensure compliance. Spain's Data Protection Act (1999) required the appointment of "security officers" when processing certain categories of data (including criminal offense-related data, credit services data, tax-related data, financial data, social security data, and 11 other types). Hungary's Act LXIII of 1992 on the Protection of Personal Data and Publicity of Public Data explicitly required DPOs in four circumstances (when processing data files of state authorities, national labor data, or national crime data; financial institutions; telecommunications service providers; and public utility service providers). Voluntary DPOs allow data controllers to decide whether to appoint a DPO based on their own circumstances, a model adopted by the UK, France, Sweden, and other countries.

2.2 Controversies Over DPO Provisions During GDPR Formulation

The EU's 1995 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 was based on automated computer processing of personal data and could no longer address various new data risks today. Since 2010, the EU began a comprehensive review of its personal data protection framework. In January 2012, the European Commission submitted the "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (hereinafter GDPR Draft) to the European Council. The GDPR Draft first incorporated DPOs into EU unified data protection legislation, and DPOs remained a focal point of legislative debate throughout the subsequent four years of negotiation and amendment.

Controversies over DPOs focused on two aspects: (1) which data controllers should appoint DPOs; and (2) whether DPO appointment should be mandatory for qualified controllers. Article 35(1) of the GDPR Draft specified three categories of data controllers that should appoint DPOs, with subparagraph (b) stating that "enterprises with more than 250 employees shall appoint a DPO." The UK, France, and other countries argued that DPO appointment should be voluntary, claiming that mandatory requirements would impose additional burdens on data controllers [9]. The UK's Information Commissioner's Office (ICO) argued that if enterprises had effective processes ensuring data

protection compliance, they need not appoint a dedicated DPO; the decision should depend on whether a DPO is necessary to achieve compliance rather than simply considering employee numbers [10]. Germany, Hungary, and other countries favored mandatory provisions, arguing they would regulate data controllers more strictly and better align with GDPR's legislative purpose. Due to these controversies, the European Parliament further raised the threshold for DPO appointment during legislative review: data controllers should appoint a DPO when processing personal data of more than 5,000 data subjects within a continuous 12-month period [11].

3. DPO Appointment and Responsibilities

3.1 DPO Appointment

3.1.1 Entities Required to Appoint DPOs Article 37(1) of the GDPR stipulates that data controllers/processors shall appoint a DPO in the following three circumstances: (1) when the data controller or processor is a public authority or body (except for courts); (2) when the core activities of the controller or processor consist of processing operations that, by virtue of their nature, scope, or purposes, require regular and systematic monitoring of data subjects on a large scale; and (3) when the core activities consist of processing on a large scale of special categories of data or data relating to criminal convictions and offenses.

(1) **Public authorities or bodies**. Article 37(3) of the GDPR provides that data controllers/processors that are public authorities or bodies shall appoint a DPO. Considering their organizational forms and government administrative costs, multiple authorities or bodies may jointly appoint a single DPO. However, data processing activities involved in courts' exercise of judicial functions are excluded from this scope.

(2) **Private enterprises or bodies**. For private enterprises or bodies, different controllers have different business scopes/purposes and thus different data processing requirements. The GDPR stipulates that enterprises whose core business is data processing and require regular, systematic, large-scale monitoring of data subjects shall appoint a DPO. In practice, multiple factors should be considered comprehensively, including the scale of the enterprise's data processing activities, duration of monitoring data subjects, and number of data subjects involved.

Given differences in national conditions and data protection policies among member states, "as the face of the enterprise, DPOs are required to be proficient in local languages and understand local realities in different countries" [12]. For multinational or cross-regional enterprise groups, it is generally accepted that the group may appoint a single DPO for multiple entities within the same country, ensuring the DPO overcomes local differences and maintains close contact with entities in different member states. For non-EU data controllers, a DPO must be appointed within the member state where the data

subject is located.

(3) **Data controllers processing special categories of data**. For data controllers or processors that process special categories of data and data relating to criminal convictions and offenses on a large scale, compliance of their data processing activities is particularly important due to the special nature of the data types, and DPOs should be appointed for strict supervision and management. Other data controllers or processors may appoint DPOs to perform corresponding responsibilities as required by EU or member state law.

3.1.2 Types of DPOs

(1) **Internal vs. External DPOs**. Based on whether the DPO is an employee of the data controller, DPOs can be divided into internal DPOs and external DPOs. DPOs need to be familiar not only with the data controller's internal data processing activities but also with its basic operations, effectively combining both. Internal DPOs are employees of the data controller, familiar with its internal operations. However, due to different previous work backgrounds, internal DPOs may lack relatively sufficient data protection knowledge and practical experience, requiring data controllers to improve their professional competence through training and other measures, which relatively increases compliance costs. External DPOs are usually professional service organizations or law firms with rich professional knowledge and practical experience. The GDPR stipulates that DPOs shall not be penalized or dismissed for performing their duties. However, internal DPOs have an employment relationship with the data controller and are likewise subject to member state labor law and corporate bylaws. If a DPO violates labor law or corporate bylaws for reasons other than performing data protection duties, the data controller may still unilaterally terminate the labor contract (unilateral termination only applies to circumstances such as serious violation of non-disclosure obligations, theft, discrimination against other employees, or other gross negligence. Generally, GDPR provisions apply, and DPOs cannot be penalized or dismissed for performing their duties). External DPOs perform their duties based on service contracts, allowing both parties to freely negotiate restrictive terms by mutual agreement, providing greater flexibility compared to internal DPOs. Typically, large enterprises choose to establish internal DPOs, while small and medium-sized enterprises mostly hire external DPOs to supervise specific data processing activities to reduce compliance costs.

(2) **Part-time vs. Full-time DPOs**. Based on whether they exclusively perform DPO work, DPOs can be divided into part-time DPOs and full-time DPOs. Part-time DPOs offer relatively flexible arrangements that can reduce data controllers' compliance costs to some extent, but conflicts arise between DPO and non-DPO responsibilities, including time allocation,

energy distribution, and conflicts of interest. Full-time DPOs are more dedicated and 更有利于 personal data protection, but correspondingly increase enterprise investment costs, which may be overly burdensome for small enterprises. In practice, data controllers should analyze specific circumstances and select appropriate DPO types, ensuring both compliance requirements are met and that the data controller can bear the costs.

3.1.3 Professional Qualifications of DPOs Article 37(5) of the GDPR stipulates that DPOs shall possess certain professional qualities, including expert knowledge of data protection law and practical operational capabilities, while being able to fulfill all DPO duties and obligations. The data protection law that DPOs need to master is not limited to the GDPR but also includes other EU regulations and member state laws related to data protection, which interact with the GDPR. DPOs should be familiar with all data processing activities of the data controller, understand its operations, and effectively combine both. Additionally, as the communication medium between data controllers, data subjects, and data protection supervisory authorities, sophisticated interpersonal skills, logical language expression capabilities, and strong public relations abilities can all effectively assist DPOs in performing their duties.

3.2 DPO Responsibilities and Their Fulfillment

DPOs play an indispensable role in ensuring relevant entities comply with data protection requirements. On one hand, DPOs must confirm data controllers' obligations, provide compliance advice, and independently monitor whether internal data processing activities comply with data protection rules. On the other hand, DPOs serve as contact points for data subjects and supervisory authorities, acting as the medium through which data subjects contact data controllers while maintaining close cooperation with supervisory authorities.

3.2.1 DPO Responsibilities

(1) **Notification and advice**. Article 39(1)(a) of the GDPR provides that to ensure data controllers and other staff obligated to implement processing activities understand their obligations and responsibilities, DPOs have a duty to inform them and provide relevant advice. For data controllers, DPOs should inform them about general data protection policies and their real-time updates; propose practical improvement measures regarding data protection to controllers or processors; and provide compliance advice on the application of data protection provisions. For other staff obligated to implement processing activities, DPOs should inform and explain general obligation issues to all employees (including administrative staff) and provide relevant advice, including their own personal data rights (while data protection obligations typically target external clients, potential clients, and other data subjects, internal employees as data subjects likewise enjoy data rights). DPOs accept consultations on any issues concerning interpre-

tation or application of provisions, 致力于提升 data controllers' and relevant personnel's data protection awareness, strengthening security during data processing operations, and reducing the risk of penalties.

(2) **Monitoring compliance of data processing**. Article 39(1)(b) of the GDPR stipulates that DPOs shall monitor compliance of internal data processing activities within data controllers. Internal data processing activities must comply not only with the GDPR but also with other EU data protection regulations, member state data protection laws, and data protection policies. DPOs should proactively monitor, assess, review, and amend relevant data protection measures [13]. DPOs may proactively or upon request directly investigate data protection-related activities within data controllers, resolve relevant issues, and report situations to the highest management level of the data controller. DPOs can conduct prior checks on data processing activities, supervise the conduct of data protection impact assessments, and provide recommendations (Article 39(1)(c) of the GDPR). DPOs should supervise employee activities, including assignment of responsibilities in data processing work, enhancement of compliance awareness, and data protection knowledge training. Internal audits (helping DPOs understand the types, locations, access rights, and complaint requests of personal data controlled by enterprises or institutions) or external audits (usually conducted by third-party organizations on specific issues such as legal or IT matters) concerning potential personal data issues and activities also fall under DPO supervision. Additionally, DPOs should appropriately consider risks that may exist in various data processing operations (Article 39(2) of the GDPR), including the nature, scope, and content of risks. Monitoring compliance of data controllers can be considered the most fundamental duty of DPOs to ensure personal data protection.

(3) **Liaising with data subjects**. Article 38(4) of the GDPR stipulates that an important responsibility of DPOs is to serve as a contact point between data subjects and data controllers. DPOs must not only master professional knowledge related to data protection but also sufficiently understand the internal situation of data controllers, including all matters and activities related to data protection. Data controllers should provide data subjects with DPO contact information to facilitate close contact between data subjects and DPOs. Data subjects may contact and consult DPOs on all issues concerning processing of their personal data and exercise of rights under the regulation.

(4) **Cooperating with supervisory authorities**. DPOs should also cooperate with supervisory authorities (Article 39(1)(d) of the GDPR), and data controllers should provide DPO contact information to supervisory authorities (Article 37(7) of the GDPR). Cooperation typically includes three aspects: (1) DPOs may serve as contact points for supervisory authorities, handling inquiries or complaints from supervisory authorities,

enabling authorities to promptly and effectively notify data controllers of relevant risks or other urgent matters; (2) DPOs may consult supervisory authorities in advance on matters related to personal data security, including audit issues, legal implementation issues, and general compliance document review issues; and (3) DPOs should supervise the implementation of recommendations proposed by supervisory authorities to data controllers and the handling of complaints, and provide timely feedback to supervisory authorities. Within their authority, DPOs may investigate and collect information on issues under review by supervisory authorities. The relationship between DPOs and supervisory authorities is one of mutual promotion—the stronger their connection, the more personal data security issues can be resolved, and the smaller the risk of rights violations.

(5) **Maintaining records and documentation of processing activities**. Article 37(1)(d) of the GDPR explicitly provides for record-keeping and documentation of processing activities. Data controllers or processors need to maintain records of all processing activities (Article 30(1) of the GDPR). DPOs are responsible for archiving records of all data processing operations. Records involve: initial information about processing, processors and third parties, principles and limitations of data processing, lawful processing conditions, personal data collections, general and special types of personal data, location of personal data, relevant security measures, collection and transmission of data, deletion and lifecycle of data, maintenance and update records of processing, role of processing, training, retention periods of records and related obligations, policies, procedures, agreements, and contracts.

(6) **Training**. Article 39(1)(b) of the GDPR explicitly provides for DPO training. DPOs need to conduct regular staff training within data controllers. The minimum training standard is to ensure all employees within the data controller understand basic data protection knowledge and have a general level of data protection awareness. More in-depth departmental training and awareness enhancement should be conducted separately according to different departments' varying data protection needs. DPOs need to continuously identify data issues that may arise in daily work of various departments and conduct data protection education for different issues in combination with departmental work scopes. Training methods may include: emails, paper documents, policy promotion, material updates, data protection courses, seminars, specific guidance, and online courses [12].

(7) **Confidentiality**. Article 38(5) of the GDPR stipulates that DPOs shall be bound by confidentiality obligations in the performance of their tasks, and shall not disclose information and documents obtained in the course of performing their duties, thereby protecting personal data and data subjects' rights.

3.2.2 Safeguards for DPO Performance To enable DPOs to better perform their duties, Article 38(1) of the GDPR provides that data controllers or processors shall ensure DPOs are properly and timely involved in all personal data protection matters and provide basic support and guarantees for their performance.

(1) **Independent status of DPOs**. The purpose of data controllers establishing DPOs is to supervise compliance of internal data processing activities, which requires DPOs to have a holistic and comprehensive understanding of data controllers' data protection policies and processing activities. Based on this, DPOs should maintain a relatively independent status within data controllers, reflected in: (1) "DPOs need a reporting line that bypasses the immediate superior to raise objections regarding relevant data processing activities" [7], meaning DPOs' reporting lines should directly reach the highest management level of data controllers or processors (see Article 38(3) of the GDPR), without direct subordinates, minimizing unnecessary interference and instructions during the reporting process—this is key to ensuring DPO independence; (2) DPOs do not belong to any department of the data controller and do not serve any specific department. DPOs need to supervise data processing activities of all departments. If DPOs were subordinate to a particular department, personal interests would conflict with enterprise interests during supervision and investigation, preventing objective performance of duties. However, this does not mean DPOs should be completely isolated from all departments—there is overlap between DPO work and other departmental work, and harmonious relationships with various departments are also important; and (3) DPOs shall not be dismissed or penalized for performing data protection duties, which constitutes performance protection for DPOs. It should be noted that DPOs' independent status is relative. The GDPR provision that DPOs "do not receive any instructions" refers to their operational independence when performing key tasks. Data controllers determine different data protection policies and implementation procedures according to the nature of different processing activities, and DPOs help data controllers achieve business objectives in compliance within this scope, freely providing compliance advice, with whether data controllers follow such advice ultimately depending on specific business standards.

(2) **Resource guarantees for DPOs**. Article 38(2) of the GDPR stipulates that data controllers shall provide DPOs with independent budgets and hardware resources as needed. Independent financial budgets ensure smooth performance of DPO duties, and DPOs may request data controllers to approve additional funding when necessary. DPOs should have access rights to personal data and processing operations in all departments, with the authority to collect personal data within data controllers and conduct prior checks on processing operations, which data controllers should support without restriction. To better perform their duties, DPOs should

have necessary resource support, such as human resources, IT resources, and office equipment. To enhance their professional competence, DPOs may request data controllers to take measures to maintain or strengthen their professional knowledge, such as organizing training and providing learning opportunities.

4. Impact of EU DPO System Implementation

4.1 Surge in DPO Demand

During the more than two-year period from GDPR's adoption on April 14, 2016, to its formal implementation on May 25, 2018, data controllers or processors subject to GDPR needed to complete compliance checklists to prepare for GDPR implementation. The most important item on the compliance checklist was DPO appointment. GDPR's increased penalties for violations undoubtedly sounded the alarm for all data controllers and processors, forcing them to appoint DPOs as required by GDPR. A study by the International Association of Privacy Professionals (IAPP) at the end of 2016 estimated the number of DPOs that would be needed: first calculating the approximate number of large EU enterprises in 13 non-financial industries, then assuming based on GDPR standards that: (1) enterprises with no fewer than 5,000 employees would "large-scale" process and monitor human resources data; (2) more than half of enterprises in transportation and warehousing, accommodation and food services, and professional, scientific, and technical services would need to appoint a DPO due to their data-intensive processing activities; and (3) all large enterprises in the communications industry would need to appoint a DPO. It also assumed that all financial institutions and insurance enterprises would need to appoint a DPO due to their business nature, while public authorities or bodies would be calculated according to EU "large enterprise" standards, assuming one DPO for every five entities requiring one. From this, the study conservatively concluded that at least 28,000 DPOs would be needed in the EU once GDPR took effect [14].

For non-EU countries, based on GDPR's definition of data controllers, any non-EU data controller that collects or processes personal data of identifiable natural persons in the EU for the purpose of offering goods or services or monitoring their activities shall be subject to GDPR, regardless of whether they are located within the EU. According to IAPP's annual privacy governance report, 50% of US enterprises need to comply with GDPR. Using trade volume estimation, with the US accounting for 17.7% of Europe's global trade, the number of DPOs potentially needed by other major European trading partners can be calculated. Estimates show that GDPR implementation will create up to 75,000 DPO positions worldwide [14].

The surge in DPO demand has created a scarcity of talent capable of filling these positions. With GDPR's implementation, a "talent war" for DPOs is underway. On one hand, the supply-demand imbalance in the job market will

drive up DPO salaries, increasing enterprise investment costs to ensure DPO professional competence and raising compliance costs. On the other hand, to increase the number of DPO professionals, training and certification institutions related to DPOs have emerged, creating a new industry.

4.2 Impact of DPO Appointment on Data Controllers and Supervisory Authorities

Establishing DPOs is significant and far-reaching for ensuring data controller compliance and reducing the burden on supervisory authorities, mainly manifested in:

4.2.1 Prior Review to Reduce Infringement Risks GDPR grants DPOs the right to conduct prior reviews. DPOs supervise the design of data processing projects, conduct advance reviews and risk assessments, reducing potential risks at the source to prevent subsequent legal sanctions, saving compliance costs for data controllers and reducing compensation expenses. Of course, supervisory authorities retain the right to investigate DPOs' reviews and assessments and verify risk prevention through investigations.

4.2.2 Optimizing Dispute Resolution Mechanisms and Reducing Supervisory Authority Burden GDPR grants DPOs the right to first handle data subject complaints. Since DPOs are more familiar with internal data protection requirements and situations of data controllers, some minor disputes and low-value claims between data subjects and data controllers can be resolved directly through DPOs. This can reduce supervisory authorities' workload to some extent, allowing them to focus on guiding and investigating serious violations while saving regulatory resources and costs. Data controllers or processors will also avoid lengthy dispute resolution procedures, improving review efficiency. Meanwhile, as the sole contact point among data subjects, supervisory authorities, and data controllers, DPOs rationalize the entire communication process, reducing unnecessary interference and conflicts.

4.2.3 Strengthening Internal Data Supervision Systems and Enhancing Data Controller Competitiveness Many links in the data processing chain may pose risks, but DPOs' detailed and comprehensive review checklists make data controllers' processing activities orderly, ensure organizational compliance, and enable clear and effective judgment of whether they are at fault as data controllers. Data protection capabilities are gradually becoming one of the standards for measuring market entity strength, and the existence of DPOs reflects both the scale of enterprise data processing and the degree of data protection, thereby enhancing market competitiveness to a certain extent.

While mandatory DPO appointment under GDPR is beneficial for the overall data protection framework, its implementation may still have some issues. Data controllers are numerous and vary in type, business scope, financial capacity,

and data protection level. A "one-size-fits-all" approach imposes restrictions on controllers that already have orderly data protection processes. Data protection rules should focus on regulating outcomes rather than processes, and DPO appointment is a preferred but not the only process control method. For data controllers meeting GDPR-specified conditions, they may already have effective data protection processes in practice, or although lacking data protection measures, their business models may limit risks within controllable scope. In such cases, mandatory DPO appointment would undoubtedly increase operational costs and waste resources. Additionally, given differences in data protection processes, development, and policies among EU member states, and that national data protection legislation had been continuously amended before GDPR to adapt to national conditions, DPOs may experience "cultural maladaptation" after GDPR's unified implementation. If negative impacts cannot be properly addressed, it will not only increase enterprise compliance costs but may even create violation risks. Therefore, many issues remain to be resolved as GDPR is formally implemented.

5. Implications of the EU DPO System for China

5.1 Implications for Chinese Enterprises

China is an important trading partner of the EU, with China-EU trade accounting for approximately 15% of the EU's global trade. GDPR implementation means Chinese enterprises also need to prepare data protection professional talent reserves and compliance readiness. While China has made significant progress in data protection research and the data industry in recent years, enterprise data protection awareness remains relatively weak, directly affecting Chinese enterprises' data protection levels and compliance capabilities. To explore European markets and conduct China-EU trade legally and compliantly, relevant Chinese enterprises should promptly conduct GDPR compliance assessments and formulate corresponding response plans to actively adapt to GDPR compliance requirements. Relevant Chinese enterprises should appoint data protection specialists (similar to DPOs) according to GDPR provisions and design a relatively complete data protection supervision process, formulating corresponding data protection and management systems.

5.1.1 Establishing Data Protection Specialist Positions Chinese enterprises can establish data protection specialist positions performing duties similar to DPOs. Personnel in these positions can provide management with advice on internal personal data collection, access, processing, transmission, and other data security issues or matters, and be responsible for supervising implementation of relevant matters. Externally, they can receive visitors and handle inquiries from users (data subjects) or third parties, providing them with available information.

5.1.2 Recording Personal Data Processing and Flow Starting from personal data collection, all uses and transfers of the personal data should be recorded. The significance lies in: (1) focusing on potential risks during the recording process to facilitate timely reporting and prevention; and (2) facilitating subsequent accountability. After personal data is infringed, responsibility subjects can be located based on records to identify non-compliant operations.

5.1.3 Establishing Data Risk Early Warning Mechanisms Data risk early warning mechanisms specifically include three aspects: pre-event risk assessment, in-process security safeguards, and post-event remediation plans. After collecting personal data, as the obligated party for data security, enterprises should take certain measures to fulfill security obligations. They shall not arbitrarily disclose, alter, or destroy collected personal data. They should appropriately adopt technical and other necessary measures to prevent personal data leakage, damage, or loss. In cases where personal data may be or has been infringed, they should immediately take remedial measures and promptly inform users and report to relevant authorities as required.

5.1.4 Strengthening Employee Training to Enhance Enterprise Data Protection Awareness An important DPO responsibility is training employees, which has more urgent needs in China. Although China's data protection has developed considerably in recent years, popularization remains low, national protection awareness is weak, and professionals are scarce. By establishing data protection specialist positions, enterprises can formulate and implement employee training plans, popularize data security knowledge within the enterprise, and enhance overall enterprise data protection awareness.

5.2 Implications for China's Data Protection System Construction

The EU is a global pioneer in data protection through specialized legislation, and its GDPR has profoundly influenced and inspired numerous countries including China. "Law alone is not enough to enforce itself." GDPR's provisions on DPO and data supervisory authority establishment and responsibilities aim to provide professional talent teams and regulatory mechanism guarantees for data subjects' rights exercise and data controllers/processors' responsibility fulfillment. GDPR was promulgated more than two years before implementation to provide a necessary transition period for relevant entities to legally equip qualified DPOs, because building professional talent and specialized institutions cannot be accomplished overnight. The EU's DPO system offers at least two implications for China's data protection system construction: (1) legislatively clarifying the obligation of data controllers/processors to establish data protection specialist positions similar to DPOs, specifying responsibilities and performance requirements for data protection specialists, and imposing corresponding accountability and penalties for non-compliant data controllers and processors; and (2) strengthening data supervisory system construction and leveraging the role of data controllers/processors' data protection specialists.

5.2.1 Clarifying Data Controllers' Obligation to Establish Data Protection Positions

(1) **Establishing data protection specialist positions and professional staffing as an obligation for data controllers and processors of certain scales and special types**. Although China's Cybersecurity Law and other relevant laws have assigned data protection responsibilities and obligations to network operators and other data controllers and processors, no provisions have yet clarified the establishment of specialized data protection positions and professionals for obligated entities. The absence of specialized positions and professionals can easily lead to discounted or ineffective implementation of laws and regulations, seriously damaging legal authority.

(2) **Clearly specifying responsibilities and performance requirements for data protection specialist positions and professionals**. The EU DPO system has clear provisions on DPO responsibilities and performance: "Public organizations (except courts), enterprises whose core business involves regular large-scale systematic monitoring of users, and enterprises whose core business involves processing sensitive personal data or personal data related to criminal offenses shall appoint a data protection officer. Multiple related enterprises may appoint one data protection officer. DPO responsibilities include informing and advising enterprises on fulfilling their obligations under GDPR, monitoring enterprise compliance, and cooperating with supervisory authorities." This largely ensures the GDPR, as a new data protection regulation, has strong operability. For such a new field as data protection, the DPO system has in fact been detailed to "what personnel (positions) to equip, what responsibilities they have, what they should do, and how to do it"—such meticulous institutional arrangements ensure effective GDPR implementation. If China can clarify responsibilities and performance requirements for data protection specialist positions and professionals in its data protection system construction, it will make obligated entities' responsibilities clear and help them fulfill their obligations transparently.

(3) **Imposing corresponding accountability and penalties for data controllers and processors with non-compliant data protection specialist appointments**. GDPR's penalty measures—enterprises violating GDPR face fines up to 4% of their global annual revenue or €20 million. Without enforcement there is no guarantee; without penalties there is no deterrence. GDPR has drawn a clear operational red line for data controllers and processors, with clear accountability and high fines directly targeting the 侥幸心理 of "lax enforcement and no accountability for violations," strictly regulating data abuse and providing strong protection for personal data. China's Cybersecurity Law establishes excessively low post-factum penalty standards that hardly serve as effective deterrence. In subsequent relevant legislation, China could draw on GDPR's account-

ability and penalty measures to strengthen regulation of data abuse.

5.2.2 Strengthening Data Supervisory System Construction and Leveraging Data Protection Specialists' Role From the above analysis of the EU DPO system, strengthening data supervisory system construction, clarifying the powers and boundaries of data supervisory authorities, and emphasizing cooperation between DPOs and data supervisory authorities are powerful measures in the EU's new data protection regulation. From the EU DPO system design, cooperation between DPOs and data supervisory authorities is crucial. Even with a well-designed DPO system, without necessary supervisory authorities and corresponding institutional arrangements, DPO functions cannot be effectively exercised. DPOs are liaisons among data subjects, supervisory authorities, and data controllers/processors, as well as task-sharers for supervisory authorities (resolving minor disputes and low-value claims). Supervisory authorities also have guidance and consultation responsibilities toward DPOs. GDPR grants data supervisory authorities investigation, correction, and penalty powers, and clarifies the division of labor and cooperation between supervisory authorities and DPOs, aiming to better protect data subjects' rights. This has important reference significance for China's ongoing exploration of data supervisory system construction, especially regarding the delineation of supervisory authorities' powers and boundaries and the regulation of division of labor and cooperation among different entities in the system.

References

[1] Xiao Dongmei. Building a Solid Data Frontier in the Global Data Torrent [N]. China Social Sciences Daily, 2016-11-10(1).

[2] Gao Fuping. International Rules for Personal Data Protection and Utilization: Origin and Trends [M]. Beijing: Law Press, 2016.

[3] LACHAUD E. Certification of Data Protection Officers Should Be Mandatory [EB/OL]. [2018-05-10]. https://ssrn.com/abstract=3176471 or http://dx.doi.org/10.2139/ssrn.3176471.

[4] MIGUEL R. Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability [J]. European Data Protection Law Review, 2017, 3(1): 114-118.

[5] Wang Rong. Big Data Era: Can the EU Rebuild a New Data Protection Order? [J]. China Information Security, 2016(1): 125-127.

[6] Zhang Min, Ma Minhu. Analysis of Development Trends in EU Data Protection Legislative Reform [J]. Chinese Journal of Network and Information Security, 2016, 2(2): 8-15.

[7] Li Xinqian. Historical Analysis and Latest Developments of German Personal Information Legislation [J]. Oriental Law, 2016(6): 116-123.

[8] CEDPO. Comparative Analysis of Data Protection Officials' Role and Status in the EU and More? I [EB/OL]. [2017-05-19]. http://www.cedpo.eu/wp-content/uploads/2015/01/CEDPO_{{{Studies}}*{{Comparative}}}-Analysis*{{{DPO}}_{{20120206}}}.pdf.

[9] MoJ Wants Obligation to Appoint Data Protection Officers Scrapped from EU Reform Proposals [EB/OL]. [2017-04-11]. https://www.out-law.com/en/articles/2013/january/moj-wants-obligation-to-appoint-data-protection-officers-scrapped-from-eu-reform-proposals/.

[10] ANGELIQUE C. Where Should the New Mandatory DPO Sit? [EB/OL]. [2017-01-21]. https://iapp.org/news/a/where-should-the-new-mandatory-dpo-sit/.

[11] European Parliament and of the Council. European Parliament Legislative Resolution of 12 March 2014 on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) [EB/OL]. [2017-07-20]. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212.

[12] China Business Wire. EU GDPR: Not Much Time Left for Chinese Enterprises [EB/OL]. [2017-03-15]. http://www.sohu.com/a/124637983_{115007}.

[13] PAUL L. The Data Protection Officer: Profession, Rules, and Role [M]. New York: Auerbach Publication, 2016.

[14] HEIMES R, PFEIFLE S. Study: GDPR's Global Reach to Require at Least 75,000 DPOs Worldwide [EB/OL]. [2017-03-20]. https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/.

Author Contributions:
Xiao Dongmei: Responsible for overall conception, drafting of some sections, and revision of the entire manuscript.
Cheng Siwen: Participated in overall planning, legal provision analysis, and drafting of some sections.

Acknowledgment of Outstanding Reviewers for *Library and Information Service* 2018

In 2018, nearly 300 reviewers participated in the peer review of manuscripts for *Library and Information Service*, reviewing over 1,400 submissions. More than 100 experts reviewed six or more manuscripts. Considering the quantity, quality, and timeliness of reviews throughout the year, 50 outstanding reviewers for 2018 have been selected (listed below). *Library and Information Service* will issue certificates to these outstanding reviewers and provide free electronic subscriptions for one year. We thank all reviewers for their strong support of *Library and Information Service*!

(Listed in pinyin order):

Name	Affiliation
Bai Rujiang	Shandong University of Technology, Institute of Science and Technology Information
Cao Jindan	Jilin University, School of Public Health
Deng Shengli	Wuhan University, School of Information Management
Deng Xiaozhao	Southwest University, School of Computer and Information Science
Fan Aihong	Tsinghua University Library
Fang Xiangming	Shanghai University Library
Feng Jia	Shanghai Academy of Social Sciences, Institute of Literature
Gao Chunmei	Sun Yat-sen University
Gao Fan	Southwest Jiaotong University Library
Gao Fuping	(Affiliation not fully specified in original)
Han Yi	Southwest University, School of Computer and Information Science
Hu Changping	Wuhan University, Center for Information Resource Research
Huang Guobin	Beijing Normal University, School of Government
Huang Linghe	Hebei University, School of Management
Jiang Chunlin	Dalian University of Technology, Faculty of Humanities and Social Sciences
Li Gang	Nanjing University, School of Information Management
Li Ming	Nanjing University, School of Information Management
Li Wu	Shanghai Jiao Tong University, School of Media and Design
Li Shuning	Beijing Normal University Library
Li Zhuozhuo	Soochow University
Liu Bing	Tianjin Normal University, School of Management
Liu Chunli	China Medical University Library

Name	Affiliation
Liu Kan	Zhongnan University of Economics and Law, School of Information and Safety Engineering
Liu Xueli	Xinxiang Medical University Journal Press / Henan Science and Technology Journal Research Center
Liu Xiaojuan	Beijing Normal University, School of Government
Liu Ziheng	Peking University, Department of Information Management
Ma Jie	Jilin University, School of Management
Ma Xueliang	National Library of China
Mao Dongmei	Jilin University, School of Public Health
Pei Lei	Nanjing University, School of Information Management
Qin Hong	University of Electronic Science and Technology Library
Ren Shuhuai	Shanghai International Studies University Library
Shao Bo	Nanjing University Library
Sheng Guangqing	Northeast Normal University, School of Information Science and Technology
Teng Guangqing	Northeast Normal University, School of Information Science and Technology
Wang Li	(Affiliation not fully specified in original)
Wang Lixue	Institute of Scientific and Technical Information of China
Wang Xiwei	Jilin University, School of Management
Wang Yanfei	Peking University, Department of Information Management
Wu Hong	Shandong University of Technology, Institute of Science and Technology Information
Wu Zhenxin	National Science Library, Chinese Academy of Sciences
Xiang Guilin	Institute of Biophysics, Chinese Academy of Sciences

Name	Affiliation
Yan Hui	Renmin University of China, School of Information Resource Management
Yang Xinya	Chongqing University Library
Zhang Guangqin	Peking University, Department of Information Management
Zhang Pengyi	Peking University, Department of Information Management
Zhang Weidong	Jilin University, School of Management
Zhao Fei	Peking University Library
Zhao Yuxiang	Nanjing University of Science and Technology
Zhu Zhongming	Lanzhou Library of Chinese Academy of Sciences / Resource and Environmental Science Information Center of Chinese Academy of Sciences

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