ChinaRxiv 中X

AI translation · View original & related papers at
chinarxiv.org/items/chinaxiv-202308.00571

The Concept, Responsibilities, and Competencies of International Data Protection Officers: Postprint

Authors: Wan Ling

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

Abstract

[Objective/Significance] This study theoretically summarizes and analyzes the meaning, types, responsibilities, and competency requirements of foreign personal data protection officers, providing academic analysis and recommendations for practical applications in China. [Methods/Process] Through retrospective literature review, this paper examines the origin and meaning of personal data protection officers; drawing upon job postings for personal data protection officers on the LinkedIn platform and the normative models of relevant occupations in the U.S. O*NET system, and based on the KSAO model and Young and Chapman's competency model, it summarizes the responsibility system and competency requirements of foreign personal data protection officers from a risk management perspective. [Results/Conclusions] Currently, foreign personal data protection officers exhibit diverse types, including both operational and advisory roles, as well as positions at both decision-making and grassroots levels. From a risk management perspective, personal data protection officers bear important responsibilities for privacy legal risk control and management. To be competent in these responsibilities, they need to possess relevant knowledge of privacy law and information analysis, demonstrate abilities such as problem sensitivity, problem-solving, and effective communication, and exhibit traits including attention to detail and adaptability to complex and fast-paced work environments.

Full Text

The Concept, Responsibilities, and Competencies of Personal Data Protection Officers Abroad

School of Management, Hebei University, Baoding 071002

Abstract: [Purpose/Significance] This paper theoretically summarizes and analyzes the meaning, types, responsibilities, and competency requirements of foreign personal data protection officers, providing academic analysis and recommendations for practical application in China. [Method/Process] Through literature review and retrospective search, we examine the origin and meaning of personal data protection officers. Referencing LinkedIn job postings for personal data protection officers and the occupational specification models of related professions in the U.S. O*NET system, and based on the KSAO model and the competency model of Yang and Chapman, we summarize the responsibility system and competency requirements of foreign personal data protection officers from a risk management perspective. [Result/Conclusion] Currently, there are diverse types of personal data protection officers abroad, including both business and consultant types, as well as both decision-level and grassroots-level positions. From a risk management perspective, personal data protection officers bear important responsibilities for privacy legal risk control. To be competent in these duties, they need relevant knowledge of privacy law and information analysis, abilities such as problem sensitivity, problem-solving, and effective communication, and traits including attention to detail and adaptability to complex and fast-paced work environments.

Keywords: personal data protection officer; privacy; competency; responsibilities

In today's society, privacy breaches and personal information trading are no longer isolated cases. An increasing number of countries and regional alliances are adopting legal and regulatory mandatory measures to govern these phenomena. The recently influential regulation is the EU's General Data Protection Regulation (GDPR), which took effect in May 2018. To comply with relevant laws and regulations, organizations, especially those involved in cross-border personal data flows, have begun establishing personal data protection officer positions and recruiting corresponding talent. For instance, numerous job postings for personal data protection officers have appeared on the international social platform LinkedIn. However, personal data protection officer is an emerging profession, and both academic research and standardized occupational classification systems lack descriptions of its job responsibilities, knowledge structure, and competency requirements. When recruiting such personnel, organizations face considerable ambiguity regarding what kind of people to hire and what responsibilities to assign them. Using LinkedIn job postings as the primary information source and referencing the occupational specification models of related professions in the U.S. O*NET system, this paper analyzes the responsibilities, knowledge structure, and competency requirements of foreign personal data protection officers from a risk management perspective, based on the KSAO model and the competency model of Yang and Chapman, providing academic analysis

for practical application in China.

1. Research Status at Home and Abroad

Unless specifically indicated, this paper generally uses "personal data protection officer" as a collective term.

Through searches on Baidu Academic (including CNKI, WOS, SCIENCE-DIRECT, and other Chinese and English databases), we retrieved over ten Chinese and foreign literature sources related to personal data protection officers. Chinese literature can be divided into two main categories: first, scholars' proposals, such as suggesting that large Chinese institutions should establish personal information or data security officer systems similar to chief privacy officers, viewing the position as an accountability mechanism to users [1-2]; second, introductions to existing domestic and foreign CPO perspectives, such as Sesame Credit's CPO viewing the role as advocating for user rights and supervising company information management systems [3], Qihoo 360's CPO viewing it as handling privacy policies, reviewing user agreements, ensuring products comply with laws and regulations, and improving privacy protection systems [4-5], Microsoft's CPO describing the work as proposing corporate data confidentiality policies, supervising user privacy protection, and training employees [6], and Dun & Bradstreet's CPO considering privacy work as an additional area of compliance work [7].

Foreign literature primarily focuses on CPO or DPO research. Many CPO studies are conducted from the perspective of helping enterprise development. For example, American scholars surveyed 11 domestic enterprise CPOs and concluded that CPOs should be privacy problem solvers, public relations communicators, and collaborators with government or legislative bodies on privacy issues [8]; Korean scholars surveyed 71 Korean organizational CPOs and found that CPOs' diplomatic roles and technical knowledge backgrounds had significant positive impacts on organizational privacy performance, while information roles, strategic roles, and legal/business knowledge backgrounds showed no significant impact [9]; J.M. Pemberton et al. noted that CPOs' most important responsibility is monitoring information systems to ensure security, making board members aware of privacy's business value, and that CPOs should have technical and humanities backgrounds, with the role's meaning continuously evolving [10]. DPO research currently mainly interprets GDPR's DPO rules, such as explaining DPO roles and status based on GDPR, emphasizing DPO independence, and stressing mastery of relevant legal, technical, and organizational management knowledge [11]; one study investigated 35 European websites' data subject access interfaces and analyzed existing problems and improvement suggestions from a DPO responsibility perspective [12].

In summary, current relevant literature is limited but spans a long publication period from 2000 to 2018, indicating the immaturity and developmental nature of this research area. Content-wise, existing research has touched upon personal

data protection officers' roles, status, and knowledge structure, recognizing that personal data protection officer is an evolving concept with increasingly complex responsibilities [13-14]. However, in-depth occupational perspective research on personal data protection officers is still lacking.

2. Origin, Meaning, and Types of Personal Data Protection Officers

2.1 Origin and Meaning of Personal Data Protection Officers

Among "personal data protection officer" categories, the Chief Privacy Officer (CPO) emerged earlier and has greater influence. According to collected data, Verizon Communications in the U.S. began appointing CPOs as early as 1994 [10], and CPOs started emerging in European and American enterprises between 1999 and 2000, defined as senior managers specifically responsible for user privacy-related matters [15]. IBM appointed its first CPO in 2001, attracting worldwide attention [16]. However, with the financial crisis's arrival and impact, this position was considered non-essential and development stagnated for about a decade. With the development and application of various information technologies such as the Internet of Things, cloud computing, and big data, especially since the EU released the "GDPR 2012 Proposal" in 2012 and formally clarified it in the 2016 GDPR, domestic and foreign enterprises have again begun emphasizing the establishment of personal data protection officer positions.

The Data Protection Officer (DPO) was first proposed by EU member states in the late 20th and early 21st centuries, with data protection laws in Germany and France both calling for this role [17-18]. The European judicial organization Eurojust released the "Eurojust Decision" in February 2002, proposing to establish DPOs within Eurojust to supervise the organization's personal data and privacy protection [19]. The EU's 2012 GDPR proposal first mandated DPO positions for global enterprises, which was formally clarified in its 2016 GDPR release. While GDPR does not define DPO, it clarifies their status and tasks within organizations: DPOs are managers who appropriately and timely participate in all personal data protection matters, responsible for supervising organizational personal data security strategies and ensuring GDPR compliance [20]. GDPR requirements are mandatory and have generated tremendous global response.

2.2 Types of Personal Data Protection Officer Positions

Between February and March 2018, we conducted multiple searches on LinkedIn's job query system using search terms "GDPR," "data protection," "Privacy officer," and "data privacy," yielding over 1,600 relevant job postings (full-time or part-time). The clustering information in the "job function" column listed various functions including sales, finance, medical services, information technology, business development, legal, management, human

resources, planning, quality inspection, consulting, analysis, customer service, and more. Such broad functional types reflect the current diverse establishment of personal data protection officer positions and that organizations typically also require personnel in other positions to assume personal data protection responsibilities.

LinkedIn categorizes all positions into executive, senior, junior, assistant, and director/supervisor levels. Table 1 shows commonly appearing personal data protection officer titles at each level:

Table 1: Personal Data Protection Officer Position Titles on LinkedIn

Position Level	Title Names
Executive	Chief Data Protection Officer, Chief Privacy Officer, Data Privacy Partner/Data Protection Officer, Partner Cybersecurity & Privacy, Data Privacy Officer & Chief Compliance Officer, Data Privacy Officer, CIO, Chief Information Security Officer, GDPR Architect, etc.
Senior	Data Privacy Project Manager, Privacy Compliance Officer, Privacy Project Manager, Data Protection Officer, Chief Privacy Officer, Privacy Manager, Security Compliance & Data Privacy Director, Security & Privacy Senior Manager, Compliance Manager, Information Governance & Security Director, GDPR Data Protection & Compliance Officer, Global Data Security Officer, etc.

Position Level	Title Names
Junior	Data Security Officer, Privacy and Security Consultant, Security and Privacy Specialist, Privacy Management Specialist, Privacy Specialist, Privacy Analyst, Privacy Director, Privacy Management Officer, GDPR Data Privacy Consultant, Privacy Director, Privacy & Compliance Officer, GDPR Information Manager, Data Protection & Privacy Management, Data Privacy Analyst, GDPR Consultant, Privacy and Data Protection, etc.
Assistant	Privacy Director, Legal Privacy Consultant, Customer Data Director, GDPR Compliance Officer, Legal Privacy Consultant, etc.

Based on LinkedIn job postings, personal data protection officer positions have three characteristics:

(1) Positions include both regulatory consultant and business types. Regulatory consultant types include legal consultant and compliance director positions. Rows 2-4 in Table 1 list business-type positions with multiple levels. Additionally, position titles containing "GDPR" appear across all five levels, highlighting GDPR's influence.

(2) Some personal data protection officer titles simultaneously include both "data" and "privacy." For example, Germany's Citco Group recruits a "GDPR?Data Privacy Officer," and U.S. Ipreo Group recruits a "Data Privacy and Security Specialist." This phenomenon shows that countries have not yet standardized occupational names for personal data protection officers.

(3) Personal data protection officers have very close relationships with compliance officers and information security officers. Compliance officers originated in the financial industry and later developed across multiple industries, with responsibilities to supervise and manage internal organizational compliance issues [21]. An important responsibility of personal data protection officers is preventing organizational violations of relevant laws, regulations, and industry norms, bearing responsibility for personal data

protection aspects of organizational compliance management. Information security officers' scope of protecting information content security includes personal data, and personal data protection officers aim to prevent personal information leakage, a protection that cannot be separated from information technology and security management.

As described above, there are many types of personal data protection officer positions, and responsibilities certainly differ across position types. Due to space limitations, the following discussion treats personal data protection officer as an occupation to examine the overall occupational responsibilities and corresponding competency requirements.

3. Responsibilities of Personal Data Protection Officers

3.1 Framework for Personal Data Protection Officer Responsibility Content

Countries typically classify mature occupations, specifying their most basic responsibilities, knowledge, skills, and ability requirements. Currently, standard systems such as the International Labour Organization's International Standard Classification of Occupations (ISCO) and the U.S. Department of Labor's O*NET online system [22] have not yet established corresponding occupations for personal data protection officers, though they list some related occupations. For example, the ISCO system includes compliance officers, CIOs, security specialists, and other related occupations, but provides minimal occupational specification content. The U.S. O*NET includes related occupations such as compliance officers, risk managers, and information security analysts, with relatively comprehensive content that can provide reference for studying personal data protection officers.

GDPR Article 39 "Data Protection Officer" specifies DPOs' most basic tasks, focusing on notification, supervision, and training of data controllers and processors regarding GDPR compliance. LinkedIn job postings for various personal data protection officers list vastly different responsibilities, but one common key responsibility is the ability to specifically implement privacy legal risk management.

This chapter will draw on relevant occupational specifications and GDPR provisions to construct a foreign personal data protection officer responsibility content framework based on risk management theory. "Risk management" refers to minimizing the probability and consequences of risk occurrence under cost constraints, including risk identification, analysis, assessment, and response planning, with the latter including risk management objective determination and risk management program planning and implementation. This concept and method have existed since ancient times, but Dr. Solomon Huebner first named it "risk management" in 1930 [23], and the theory and method are now widely applied. Based on GDPR provisions for DPOs and LinkedIn personal data protection officer job postings, the essence of personal data protection officers is privacy legal

risk management and preventing organizational violations of relevant laws and regulations. Therefore, we summarize foreign personal data protection officer job responsibilities based on risk management theory and methods, as shown in Figure 1 [Figure 1: see original paper].

3.2 Analysis of Personal Data Protection Officer Responsibility Content

(1) **Identify, analyze, and evaluate privacy legal risks.** In personal data protection, organizational risks mainly include legal risks and operational risks. Legal risk refers to organizations being legally or industrially sanctioned for violating relevant laws, regulations, and industry norms; operational risk refers to organizations falling into difficulty due to failure to effectively prevent user or employee personal data leakage, such as declining business reputation and customer loss. This paper focuses on personal data protection officer responsibilities under the first risk type. Specific content includes: determining the basis for identifying and analyzing privacy risks, identifying and analyzing privacy legal risk types, occurrence probability and consequences, occurrence stages and triggering factors, evaluating risk impact levels, and prioritizing handling order. When conducting this work, attention must be paid to: monitoring updates to relevant laws and regulations; analyzing the sources of risk problems; paying attention to the security of various information technologies and equipment. Clearly, to fulfill these responsibilities, personal data protection officers must work closely with other organizational personnel (such as compliance officers, information security officers, CIOs, business departments, and IT technicians).

(2) **Assist in formulating privacy legal risk management objectives.** Risk management objectives include three types: avoidance, transfer, and response. Risk avoidance means organizations abandon collecting personal data and consequently must forgo benefits obtainable from using personal data. Risk transfer means transferring risk to third parties through cooperation or to users through exculpatory contracts. For example, in January 2018, Apple emailed its users stating it had stored Chinese mainland customers' personal data in Guizhou-Cloud Big Data. While Apple's practice was to comply with Chinese legal requirements, it also partially transferred personal data storage security risk to Guizhou-Cloud Big Data. Risk response means retaining risk and taking measures to control and channel risk-triggering factors, with specific content covered in (3)-(6) below. Since risk management objective determination actually corresponds to organizational overall objectives, it should be decided by the organization's top decision-makers, with personal data protection officers mainly providing staff advice and legal consultation.

(3) **Plan privacy legal risk management content.** The main form is developing privacy policies, including "privacy policies" for users and pri-

vacy legal risk management policies for internal organizational and partner employees to follow. User-facing "privacy policies" should be written in language that is clear, understandable, and consistent with user privacy cognition. For internal-facing policies, two points need attention: much personal data leakage currently occurs internally, requiring policy content to improve internal personal data protection authority and procedures; ensuring partner organizations' personal data protection policies meet the organization's requirements, which becomes increasingly important as various outsourcing businesses grow [24].

(4) **Deploy and supervise privacy legal risk management implementation.** Policy execution requires standardized processes for implementation and promotion. Risk management implementation plans typically include: unifying thinking, i.e., establishing organizational personal data protection culture and climate; decomposing management activities, i.e., clarifying employee-position responsibility matching; organizational preparation, i.e., building a personal data protection organizational system including personnel and departments; implementation means, i.e., promoting and supervising personal data protection implementation through training and daily consulting services, and through periodic inspections and handling privacy leakage complaints.

(5) **Participate in privacy legal risk management assessment.** Large enterprises or financial industries typically conduct compliance management work with annual compliance assessments. As part of or closely related to compliance management, privacy legal risk management requires participation in organizational compliance assessments. Personal data protection officers need to submit privacy legal risk identification results, privacy legal risk management plans, and privacy legal risk incident reports to compliance officers, auditors, or general counsel. Additionally, as assessors, personal data protection officers must conduct privacy legal compliance audits of organizational business activities and supervise the compliance of new technology and big data usage.

(6) **Interface with regulatory authorities and users.** Personal data protection officers are the external contact points for organizational personal data protection activities [25]. Interfacing with regulatory authorities requires clear and correct understanding of regulatory requirements and accurate and timely reporting of organizational measures and existing problems to regulators. Interfacing with users includes accepting user complaints about privacy leakage, recording, tracking, investigating, and preventing continued leakage, and handling aftermath work. When interfacing with users, contact information should first be clearly displayed on websites or software. Currently, research shows that when European researchers access European websites to find data controller contact information, it takes an average of 4.5 minutes, with only a 70% success rate via internet search [12], reflecting that organizations are currently

not doing well in user interfacing.

4. Competency Requirements for Personal Data Protection Officers

This section analyzes current foreign personal data protection officer competency requirements based on the commonly used human resources KSAO model. Here, K represents knowledge, S represents skills, A represents abilities, and O represents other factors, primarily referring to personal attitudes and traits [26]. Currently, LinkedIn job postings and U.S. O*NET system occupational specification content basically apply the KSAO model.

4.1 Knowledge and Skills Requirements

Personal data protection officer knowledge and skills should target fulfilling the position's responsibilities. Based on Section 3 content, we can summarize the following key knowledge and skill requirements:

(1) **Relevant laws, regulations, and industry norm knowledge.** From a risk management perspective, the core of personal data protection officers is resolving privacy legal risks; therefore, legal knowledge and industry norm knowledge are essential professional knowledge. Most chief privacy officer recruitment information collected from LinkedIn requires a law doctorate, demonstrating that legal knowledge is the most fundamental knowledge requirement for this profession.

(2) **Foreign language knowledge.** In the internet environment, personal data subject users are likely spread globally, requiring personal data protection officers to handle privacy legal risk complaints from different countries. Foreign language knowledge is indispensable, especially English listening, speaking, reading, and writing skills that should reach a certain level.

(3) **Information technology knowledge and information tool usage skills.** Currently, personal data collection, storage, and processing rely more on information technologies and tools. Mastering these technologies and tools enables personal data protection officers to more keenly identify and analyze privacy legal risks.

(4) **Other relevant knowledge and skills.** Personal data protection officers belong to management occupations and should master basic management knowledge. Additionally, personal data protection officers need to communicate with business departments to cooperate on personal data protection and should master basic industry knowledge. For example, personal data officers in the information services industry should understand information services business knowledge, while those in the financial industry should understand financial business knowledge.

4.2 Ability and Other Trait Requirements for Personal Data Protection Officers

For mature occupations, national occupational classification systems provide key ability requirements. Currently, the O*NET system includes related occupations such as compliance officers, risk managers, information security analysts, and security management managers. The system provides abilities, occupational interests, work values, and work styles for each occupation, with the latter three corresponding to the O (other factors) in the KSAO model. Common abilities across these related occupations mainly include: problem sensitivity, reasoning ability (deductive and inductive), expression ability, comprehension ability, detail observation ability, classification flexibility, and information ordering ability. Other trait requirements mainly include: attention to detail, critical thinking, integrity and reliability, independence, initiative, cooperativeness, stress resistance, and persistence.

This paper focuses on discussing the management functions of dedicated information services industry personal data protection officers. Therefore, we further limited the over 1,000 records mentioned in Section 2.2 to those with position titles containing "privacy," "data," or "GDPR," obtaining 35 valid statistical sources. Among them, the numbers of job postings at executive, senior, junior, assistant, and director/supervisor levels are 9, 12, 6, 7, and 1, respectively. These job postings have diverse requirements for abilities and traits with varied language expressions. Through concept extraction, we first identified 86 ability and trait concepts, then further refined and summarized them into 20 abilities (see Figure 2 [Figure 2: see original paper]). In addition to particularly emphasizing "communication ability," executive and director/supervisor levels also emphasize management ability, senior and assistant levels emphasize analytical ability, while junior levels value expression ability.

Comparing O*NET and LinkedIn ability and other quality requirements, both attach great importance to communication ability and analytical ability. Relatively speaking, LinkedIn job postings emphasize communication ability more, while barely mentioning problem sensitivity. From a privacy legal risk management perspective, problem sensitivity and problem-solving ability are very important. Additionally, four job postings emphasize personal data protection officers' business awareness. Drawing on the above summarized ability types and comprehensively considering Section 3 content, we use Yang and Chapman's competency model, which includes basic abilities, cognitive understanding abilities, personal skills, interpersonal abilities, work matters, and others [27-28], to analyze foreign personal data protection officer ability requirements. Here, we primarily organize according to the latter five categories:

(1) **Basic abilities** mainly include expression ability (oral and written) and technology application ability.

(2) **Cognitive understanding abilities** mainly include problem sensitivity, reasoning and analysis ability, evaluation ability, information management

ability, risk element ordering ability, problem-solving ability, and learning ability.

(3) **Interpersonal abilities** mainly include communication ability, collaboration and cooperation ability, interpersonal skills, and relationship management ability.

(4) **Work matters** mainly include influence, leadership, and training ability. These abilities help personal data protection officers improve work efficiency and quality, with the first two being essential for senior-level personal data protection officers. "Training ability" is a key capability for personal data protection officers to fulfill their "enabler" role.

(5) **Other aspects such as traits** mainly include: stress resistance, ability to adapt to complex and fast-paced work, time management, attention to detail, independence, and integrity. Personal data protection officer responsibilities are essentially control functions, often facing pressure from both regulatory requirements and business development, with complex environments where privacy legal risks exist in many work details. Therefore, they must not only have problem-solving ability but also withstand these pressures and strongly adapt to complex and fast-paced environments.

Currently, some professional certificates related to personal data protection have emerged in the market to measure whether individuals possess personal data protection officer qualifications. Examples include the International Association of Privacy Professionals (IAPP)'s CIPP (Certified Information Privacy Professional), CIPM (Certified Information Privacy Manager), and CIPT (Certified Information Privacy Technologist), as well as healthcare industry certifications such as CHPS (Certified in Healthcare Privacy and Security) and HCISPP (HealthCare Information Security and Privacy Practitioner).

5. Implications for Developing the Personal Data Protection Officer Profession in China

5.1 Actively Deploy Personal Data Protection Officer Positions Within Organizations

China has increasingly emphasized personal information protection in recent years, successively issuing the Criminal Law Amendment, Cybersecurity Law, and other legislation that strengthens personal information protection, while providing specific guidance to organizations through standards such as "Information Security Technology - Personal Information Security Specification." Against this backdrop, some Chinese enterprises have begun establishing personal data protection officer positions. For example, Qihoo 360 and Sesame Credit established CPO positions in 2012 and 2016, respectively, while China Eastern Airlines, High-Tech Group, and Huawei established DPO positions, GDPR audit expert positions, and privacy engineering technology expert positions in 2018. However, whether viewed from LinkedIn job postings or Baidu search infor-

mation, very few domestic Chinese enterprises have established personal data protection officer positions. From a development trend perspective, all types of Chinese organizations should actively carry out personal data protection officer position system establishment work.

5.2 Emphasize the Privacy Risk Control Role of Personal Data Protection Officers

From domestic and foreign scholar research and current LinkedIn job posting status, more and more organizations recognize personal data protection officers' role in preventing privacy legal risks. However, the uneven job posting content shows that some organizations still pay insufficient attention to privacy risk control, overemphasizing external communication responsibilities that actually stress public relations functions—a phenomenon worth contemplating. When Chinese enterprises establish personal data protection officers, their responsibility planning should strengthen privacy risk prevention and control requirements, which serve as an important driving force for organizations to actively implement personal data protection measures.

5.3 Strengthen Personal Data Protection Officer Talent Cultivation and Authoritative Certification

When Chinese organizations plan personal data protection officer types, positions, responsibilities, and competency requirements, they can draw on the above foreign experiences and establish certifications similar to CIPP, CIPM, and CIPT. At the "Second China Data Security Governance Summit Forum" held in Beijing in May 2018, participants expressed hope that the newly established "China Cybersecurity and Informatization Industry Alliance Data Security Governance Committee" would undertake (personal data) security talent competency certification work. Such certification work helps cultivate authoritative personal data protection officer talent. Additionally, foreign markets have begun emerging consulting services providing DPO solutions, such as the "ESOMAR Plus Service" offered by the European Society for Opinion and Marketing Research [29], and China could also develop similar consulting services to help various organizations design their personal data protection officer positions from a professional perspective.

In conclusion, as an emerging profession, the role personal data protection officers play within organizations, the responsibilities they undertake, and the knowledge structure and competency qualities they require all need continuous planning and improvement through practice and research, while also urgently needing domestic and international industry experience exchange and mutual learning.

References

[1] Zhou Qingshan. Reflections on improving China's personal information

protection management system [J]. Social Governance, 2018(1): 34-41. [2] Zhan Xinhui. Chief Privacy Officer [J]. Young Journalist, 2011(7): 85. [3] Nie Zhengjun. Data security in the eyes of the chief privacy officer [J]. Hangzhou (Weekly), 2017(17): 28-29. [4] He Jun. Qihoo 360 first establishes "Chief Privacy Officer": Privacy protection should change from "luxury" to "necessity" [N]. Securities Daily, 2012-03-21(D02). [5] Hu Xiaohe. "Multi-role player" discusses information security protection strategies in the big data era—Interview with Tan Xiaosheng, Chief Privacy Officer and Vice President of Qihoo 360 Technology Co., Ltd. [J]. Information Security and Communications Privacy, 2016(11): 87-91. [6] Xin Wen. CPO prevails in the IT era [N]. Factory Manager Daily, 2001-07-20(A03). [7] Association of Corporate Counsel. Dun & Bradstreet Chief Privacy Officer and Senior Compliance Advisor Aryeh Friedman: The successful way to address compliance challenges [J]. Legal Person, 2012(5): 20-22. [8] AWAZU Y, DESOUZA K C. The knowledge chiefs: CKOs, CLOs and CPOs [J]. European management journal, 2004, 22(3): 339-344. [9] WEE J, MA S, KIM S. The impact of chief privacy officers' background knowledge and role on organizational privacy performance [EB/OL]. [2018-06-17]. http://iieng.org/images/proceedings_{pdf}/9571E0214076.pdf. [10] PEMBERTON J M. Chief privacy officer: your next career? [J]. The information management journal, 2012, 36(3): 57-58. [11] PAULL. The data protection officer profession, rules, and role [M]. Boca Raton: Taylor & Francis Group, 2016. [12] LHOIRY X D, NORRIS C. The honest data protection officer's guide to enable citizens to exercise their subject access rights: lessons from a ten-country European study [EB/OL]. [2018-06-17]. http://eprints.whiterose.ac.uk/86163/. [13] Editorial Department. Is the chief privacy officer just a flash in the pan? [N]. Computer World, 2006-03-20(B15). [14] DIMICK C. The new privacy officer [J]. Journal of AHIMA, 2012, 83(4): 20-25. [15] Editorial Board. Another emerging network position: CPO [J]. Computer & Network, 2000(21): 34. [16] Editor. IBM creates world's first privacy officer [J]. Computer Applications in Petroleum Industry, 2001(1): 52. [17] Gao Fuping. International rules for personal data protection and utilization: Origin and trends [M]. Beijing: Law Press, 2016. [18] Li Xiaohui. Germany has advantages in personal data protection [J]. China National Conditions and Strength, 1997(12): 41. [19] EUROJUST. Council decision [EB/OL]. [2018-02-22]. http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ejdecision/Eurojust%20Decision%20(Council%20Decision%202002%20187%20JHA)/Eurojust-Council-Decision-2002-187-JHA-EN. [20] EU. General data protection regulation [EB/OL]. [2018-02-20]. http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf. [21] Cai Ningwei. Chinese and foreign comparison of bank chief compliance officers—Based on importance, necessity, and feasibility analysis [J]. Southwest Finance, 2017(11): 59-64. [22] U.S. Department of Labor. O*NET OnLine [EB/OL]. [2018-03-10]. https://www.onetonline.org. [23] Sun Lixin. Risk management [M]. Beijing: Economic Management Press, 2014: 23. [24] AWAZU Y, DESOUZA K C. The knowledge chiefs: CKOs, CLOs and CPOs [J]. European management journal, 2004, 22(3): 339-344. [25] TIKKINEN-PIRI C, ROHUNEN A, MARKKULA J. EU general data

protection regulation: Changes and implications for personal data collecting companies [J]. Computer law & security review, 2018, 34(1): 134-153. [26] Song Jingqi. Research on competency-based human resource management [J]. China Management Informationization, 2015, 18(12): 95. [27] YOUNG J, CHAPMAN E. Generic competency frameworks: A brief historical overview [J]. Education research and perspectives, 2011, 37(1): 1-24. [28] Du Ruijun, Zhou Tingyong, Zhou Zuoyu. Construction of college student competency model: Concept, coordinates, and principles [J]. Education Research, 2017, 38(6): 44-57. [29] KIM S. Designating a data protection officer [J]. Research world, 2017(63): 38.

Wan Ling School of Management, Hebei University, Baoding 071002

The Concept, Responsibility and Ability of Personal Data Protection Officer Abroad

Abstract: [Purpose/significance] This paper summarizes and analyzes the meaning, type, responsibility and ability quality requirements of foreign personal data protection officers in theory, and provides academic analysis and suggestions for the application in China's practice field. [Method/process] Through literature backtracking retrieval, the origin and meaning of personal data protection officers are examined. Referring to the recruitment announcements of personal data protection officers on the LinkedIn platform and the normative models of related occupations in the US O*NET system, based on the KSAO model and the competency model of Yang and Chapman, the responsibility system and competency requirements of foreign personal data protection officers are summarized from the perspective of risk management. [Result/conclusion] At present, there are various types of personal data protection officers abroad, including business types and consultant types, as well as decision-making and grassroots levels. From the perspective of risk management, personal data protection officers undertake important responsibilities for privacy legal risk control. To be competent for these responsibilities, they need to have corresponding privacy legal knowledge, information analysis knowledge, etc., should have the ability to be sensitive to problems, solve problems, and be good at communication, and should have the characteristics of paying attention to details and adapting to complex and fast-paced work environments.

Keywords: personal data protection officer; privacy; competency; responsibilities

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

Source: ChinaXiv — Machine translation. Verify with original.