EXEMPTION RULES IN CHINA'S NEW REGULATION ON CROSS-BORDER TRANSFER OF PERSONAL INFORMATION[*]

Zhiheng NIU[**]

Table of Contents

[*] This Article is one of the research outcome of the National Social Science Foundation's key project "Research on Trade by Internet and Protection of Civil Rights (互联网交易制度和民事权利保护研究)" (Project No. 20 & ZD 192).

[**] Zhiheng NIU, PhD Student at School of Law, Tsinghua University.

EXEMPTION RULES IN CHINA'S NEW REGULATION ON CROSS-BORDER TRANSFER OF PERSONAL INFORMATION

Zhiheng NIU

Abstract

China's newly issued Provisions on Promoting and Regulating Cross-border Data Flow clarifies under which circumstances can the data processor be exempted from the preconditions stipulated in Article 38 of Personal Information Protection Law. The scope and extent of the exemption rules reflect China's data outflow attitude and the justifications behind the rules need to be explored and constructed. Justifications behind the exemptions rules differ: while data transit is justified both on the low risk of transit itself and the data classification and grading policy, exemptions under specific situations can find the counterparts in General Data Protection Regulation and transcend the relatively conservative regulation patterns.

Keywords: Cross-border; PCDF; Transfer of personal information; PIPL.

I. INTRODUCTION

Cross-border data transfer is the basis for global communication and exchange of information, technologies, goods, etc. Promoting cross-border data transfer under the prerequisite of national security is conducive to fully exploring the value of data and developing new productive forces.[1] Pursuant to Article 38 of Personal Information Protection Law (hereinafter "PIPL"), promogulated in 2021, where a personal information processor truly needs to provide personal information to any party outside the territory of the PRC due to business or other needs, the processor shall meet either of the following conditions: (1) the processor has passed the security assessment organized by the national cyberspace administration in accordance with Article 40 of PIPL; (2) the processor has achieved the personal information protection certification from professional institutions pursuant to the regulations by the national cyberspace administration; (3) the processor has entered into a standard contract formulated by the

[1] *See* Cujin he Guifan Shuju Kuajing Liudong Guiding Da Jizhe Wen (《促进和规范数据跨境流动规定》答记者问) [Remarks on Provisions on Promoting and Regulating Cross-border Data Flow], Cyberspace Administration of China, Website (Nov. 11, 2024), https://www.cac.gov.cn/2024-03/22/c_1712776611649184.htm.

national cyberspace administration; (4) the processor has met other conditions provided in laws, administrative regulations, or rules laid down by the national cyberspace administration.[2] Article 38 of PIPL articulates the requirements of the cross-border transfer of personal information (hereinafter "transfer of personal information"), aiming at achieving a reasonable balance between the protection of personal rights, social order and national security, and the need of data transfer for transnational commerce, cultural and academic exchanges, development of digital economy, etc.[3]

On March 22, 2024, Cyberspace Administration of China issued the Provisions on Promoting and Regulating Cross-border Data Flow (hereinafter "PCDF"),[4] which contains certain exemption rules within specific circumstances to the requirements of transfer of personal information under Article 38 of PIPL, in turn adding flexibility to Article 38 of PIPL and facilitating the transnational data flow. Exemptions from the duties regulated in Article 38 of PIPL (hereinafter "Exemptions") exist where the transfer of personal information only constitutes a data transit (Article 4 of PCDF) and where the transfer takes place in specific circumstances (Article 5 of PCDF). Policy considerations and justifications behind the two exemption rules are to be analyzed and a more detailed elaboration of the application of the exemption rules is to be constructed. Chapter II will analyze Article 4 of PCDF concerning data transit, and Article 5 of PCDF will be analyzed in Chapter III.

II. DATA TRANSIT: CHINA'S NEW VERSION

Article 38 (1) of PIPL articulates that, transfer of personal information refers to situations where personal information processor transfers the personal information to parties outside the territory of the PRC. Nevertheless, whether data transit falls within the scope of Article 38 remains in doubt.

Before PCDF comes into existence, there are already academic opinions stating that if certain data flows only transit through China without any modifications or processes, these data flows cannot be

[2] Geren Xinxi Baohu Fa (个人信息保护法) [Personal Information Protection Law] (promulgated by the Standing Comm.13th Nat'l People's Cong, Aug. 20, 2021, effective Nov.1, 2021) Art. 38, STANDING COMM.13TH NAT'L PEOPLE'S CONG (China).

[3] *See* Cheng Xiao (程啸), Geren Xinxi Baohu Fa Lijie yu Shiyong (个人信息保护法理解与适用) [Understanding and Application of Personal Information Protection Law], 305-306 (2021).

[4] *See* Cujin he Guifan Shuju Kuajing Liudong Guiding (促进和规范数据跨境流动规定) [Provisions on Promoting and Regulating Cross-border Data Flow] (promulgated by the Cyberspace Administration of China, Mar. 22, 2024, effective Mar. 22, 2024), CYBERSPACE ADMINISTRATION OF CHINA (China).

regarded as a "transfer" but only a "transit".[5] Article 3 of exposure draft of PCDF also signifies if the personal information being transferred is not collected inside PRC, the data processor shall be exempt from applying for a security assessment of cross-border data transfer, concluding a standard contract for the transfer of personal information, or passing a personal information protection certification. A counter part of the rules in exposure draft of PCDF can be found in Singapore's Personal Data Protection Regulations 2021, which introduces specific rules to the application of Singapore's Personal Data Protection Act 2012. According to Article 9 of Singapore's Personal Data Protection Regulations 2021, data in transit means personal data transferred through Singapore in the course of onward transportation to a country or territory outside Singapore, without the personal data being accessed or used by, or disclosed to, any organization other than the transferring-organization itself while the personal data is in Singapore, except for the purpose of such transportation.[6]

A. Beyond Mere Transit

In contrast, Article 4 of PCDF follows a different legislative pattern, which allows the data processor to enjoy Exemptions when the data processor, during the processing, does not introduce any personal information or important data generated inside China.[7] A typical situation where this Article applies is the data processing business in Hainan Province, where many enterprises undertake business of processing the data importing from other countries and then exporting them back after processing. In February 2024, A "Digital Bonded Zone" in Danzhou, Hainan passed the acceptance inspection, and the data processing enterprises in the zone can provide value-added services such as processing, management, and trading for imported data, and then export the processed products back to the foreign countries where the data is collected or generated.[8]

In theory, if the data processors in China only provide data transit service without any processing, allowing them to enjoy the Exemptions has sufficient ground of justification, because the simple transit does involve any personal information and data collected inside China.[9] Nevertheless, an opposing interpretation of Article 4 of PCDF suggests

[5] *See* Long Weiqiu (龙卫球), Zhonghua Renmin Gonghe Guo Geren Xinxi Baohu Fa Shiyi (中华人民共和国个人信息保护法释义) [Explanation of China's Personal Information Protection Law] 182 (2021).

[6] Singapore's Personal Data Protection Regulations 2021, Article 9.

[7] PCDF, Article 4.

[8] *See* Wu Xinyi (吴心怡), *Hainan Ruhe Chengshu Ershang* (海南如何乘"数"而上) [*How can Hainan develop by digitalization*], HAINAN RIBAO (海南日报) [HAINAN DAILY], Apr. 10, 2024, at A05.

[9] *See* Cheng Xiao (程啸), Shuju Quanyi yu Shuju Jiaoyi (数据权益与数据交易) [Data Rights and Data Transaction] 519 (2024).

that the data processor is allowed to have Exemptions when introducing data which does not qualify as "important data", and contains no personal information during the processing.

B. Theoretical Basis

A comparative view of EU's General Data Protection Regulation (hereinafter "GDPR") can be made, where no definition of data transfer has been clarified in Chapter V, which handles with the transfer of personal data outside EU to other countries. GDPR does not differentiate between data transfer and data transit, but dealing all kinds of data outflow using the concept "data transfer".[10] Reason behind EU's unified treatment of data transfer and transit lies in the fact that the boundaries between them is becoming increasingly blurred, which leads to a practical difficulty in distinguishing these two types of data outflow. But the difficulty in differentiating does not mean a mere data transit should be treated in the same way as data transfer in the narrow sense. When assessing the risks caused by data outflow, consideration should be taken that a mere transfer of data will not cause a substantial risk to the interests protected by GDPR.[11]

When Article 4 of PCDF is analyzed in the view of the potential risks caused by transit, the theoretical basis lies in the measuring of potential risks emerging during data outflow. In 2022, Cyberspace Administration of China issues Measures for the Security Assessment of Outbound Data Transfer, Article 5 of which requires the data processor to assess the legality, legitimacy, and necessity of the data outflow's purpose, scope, and method, and size, scope, type, and sensitivity of the data to be transferred which may endanger national security, public interest, or the lawful rights and interests of individuals or organizations.[12] From this Article the attitude of regulation of data outflow can be summarized as emphasizing the legality, necessity and the risks during the outflow. A further elaboration expression of this Article can be found in China's data classification and grading policy.

The National Technical Committee 260 on Cybersecurity of Standardization Administration of China launches Data security technology — Rules for data classification and grading on March 15, 2024, which grades data into three kinds, including core data, important

[10] SVETLANA YAKOVLEVA, GOVERNING CROSS-BORDER DATA FLOWS: RECONCILING EU DATA PROTECTION AND INTERNATIONAL TRADE LAW 39 (2024); EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

[11] CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW, OXFORD UNIVERSITY PRESS 174-175 (2013).

[12] Shuju Chujing Anquan Pinggu Banfa (数据出境安全评估办法) [Measures for the Security Assessment of Outbound Data Transfer] (promulgated by the Cyberspace Administration of China, Jul. 7, 2022, effective Nov. 1, 2022), CYBERSPACE ADMINISTRATION OF CHINA (China).

data, and general data in a sequence of significance. Core data refers to those "important data with high coverage, precision, scale, and depth in a field, group, or region that, if illegally used or shared, may directly affect political security". Important data refers to those "data in specific fields, groups, regions, or with a certain level of accuracy and scale that, once leaked, distorted, or damaged, may directly endanger national security, economic operation, social stability, public health, and safety". Other data not falling into the category of key data or important data is classified as general data, and those data only concerning individual interests or enterprise's interests belongs to general data in principle.[13] The outflow of core data and important data has nothing to do with Exemptions, because the general interest of the country and society is in a high possibility of being seriously harmed if these kinds of data are exempted from ex ante assessment or security checks. Quite the contrary is the attitude towards the general data, since the outflow of general data in principle only involves the interest of private entities, the necessity of supervising and regulating is relatively lower comparing with the aforementioned core data and important data. A policy towards free flow of the general data is preferred.[14]

As to the contextual meaning of Article 4 of PCDF, data transit is regarded and presumed by the drafter of PCDF as not posing risks to the interests protected by PIPL in the scene of transfer of personal information, and the general data added to the data during the part of transit inside the territory of China will not cause great risks to national security and personal rights. Consequently, the justification of Article 4 of PCDF lies in the classification and grading of data, which clarifies that risk of general data's outflow can be tolerated, thus the data processor can enjoy the Exemptions.

Furthermore, there is an academic opinion expressing concerns that although the requirement of Article 4 of PCDF is satisfied, the processing of data introduces neither personal information nor important data, but the outcome of the processing may make the data hazardous to national security or social interest. Under these circumstances, whether all kinds of data transit enjoy Exemptions

[13] Shuju Anquan Jishu Shuju Fenji Fenlei Guize (数据安全技术数据分类分级规则(GB/T 43697-2024)) [Data Security Technology — Rules for Data Classification and Grading] (promulgated by the National Technical Committee 260 on Cybersecurity of Standardization Administration of China, Mar. 15, 2024, effective Oct. 1, 2024), NATIONAL TECHNICAL COMMITTEE 260 ON CYBERSECURITY OF STANDARDIZATION ADMINISTRATION OF CHINA (China), Article 3.2 and 3.3。

[14] *See* Hong Yanqing (洪延青), *Guojia Anquan Shiye Zhongde Shuju Fenlei Fenji Baohu* (国家安全视野中的数据分类分级保护) [*Data Classification and Hierarchical Protection in the Vision of National Security*], 5 ZHONGGUO FALV PINGLUN (中国法律评论) [CHINA LAW REVIEW] 71, 76 (2021).

remains in doubt.[15] This concern must not necessarily be related to the exemption rules regulated in PCDF, and a better approach should be that during the phase of data import, relevant assessing measure are taken over the data content and purpose of processing to ensure the processing itself will not be against law and regulations, which is an obvious explanations of rules not confined to data area.

III. EXEMPTIONS IN SPECIFIC CIRCUMSTANCES

Article 5 of PCDF articulates that a data processor enjoys Exemptions during transfer of personal information, in so far the personal information does not contain any important data, under circumstances including: (1) personal information must be provided to an overseas recipient as needed for the conclusion or performance of a contract to which the individual is a contracting party, such as cross-border shopping, delivery, remittance, payment, and account opening, booking of air tickets and hotels, visa application, and exam services; (2) personal information of any internal employee must be provided to an overseas recipient as needed for human resource management under the labor rules and regulations developed in accordance with the law and a collective contract signed in accordance with the law; (3) personal information must be provided to an overseas recipient to protect the life, health, or property safety of natural persons under emergency circumstances; (4) Data processors, other than operators of critical information infrastructure, have cumulatively provided personal information (excluding sensitive personal information) to foreign countries for fewer than 100,000 individuals since January 1 of the current year.[16] The first three circumstances of Exemptions can find counterparts in Article 49 of GDPR, the derogations for specific situations. It is important to mention that the word usage of the first three circumstances is similar to Article 13 of PIPL which deals with certain situations where data processor can process personal information with or without the consent of the personal information subject, especially where there exists no consent. Nevertheless, the purpose of Article 13 of PIPL and Article 5 of PCDF is different: the former deals with the process while the latter deals with the transfer of personal information. Justifications and rationales behind Article 13 of PIPL cannot, at least, directly apply to Article 5 of PCDF. The fourth circumstance is a new policy in the area of transfer of personal

[15] *See* Liu Jinrui (刘金瑞), *Shuju Kuajing Shuanggui Zhixia Geren Xinxi Chujing Jianguan Huomian Zhidu de Shiyong yu Wanshan* (数据跨境双轨制下个人信息出境监管豁免制度的适用与完善) [*Application and Improvement of Exemption System from Supervision on Outbound Transfer of Personal Information under the Dual-track System for Cross-border Data*], 5 CAIJING FAXUE
(财经法学) [LAW AND ECONOMY] 23, 31 (2024).

[16] PCDF, Article 5.

information from a comparative view. The justification for all four circumstances illustrated in Article 5 of PCDF will be analyzed separately in this part.

A. Exemptions for Performance of Contract

If the data subject is one contract party, and the data processor is the other party, and the data processor must transfer the personal information to ensure the performance of contract, what justifies the data processor's entitlement to Exemptions?

Article 49 (1) (b) of GDPR has a similar formulation as Article 5 (1) (1) of PCDF, articulating that the transfer must be necessary to the performance of contract in order to be viewed as a justified derogation of GDPR's data transfer requirements. Since Article 49 (1) (b) of GDPR can be traced back to Article 26 (1) (b) of Data Protection Directive,[17] materials explaining the rules in Data Protection Directive also worth to be referred. According to the legislative intent of Data Protection Directive, the derogation rules is set to satisfy the requirement of international trade and add flexibility to transfer of personal information.[18]

Under GDPR, firstly, it is a contract-based derogation which can only be raised in occasional transfers of data instead of a systematic, repetitive data transfer where the data transfer takes place within a stable relationship.[19] Secondly, "necessary" means that between the data subject and the purpose of the contract must exist a close and substantial connection, e.g., if the data processor provides personal information to recipients outside EU to perform a contract like cross-border shopping, hotel booking, car renting, etc., derogation of GDPR is allowed when the contract cannot be performed with the personal information being transferred.[20] As a consequence, Article 49 (1) (b) of GDPR cannot serve as a justification for the transfer of additional information which is not transferred for the purpose of performance of the contract.[21] The narrow understanding of Article 49 (1) (b) of GDPR can be viewed as a method of achieving a relatively conservative balance between protection of fundamental rights cherished by EU and the practical needs of international trade and the narrow understanding itself can be viewed as a justification of the rule.

[17] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[18] Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, 2093/05/EN WP 114, at 7.

[19] TOBIAS NAEF, DATA PROTECTION WITHOUT DATA PROTECTIONISM 152 (2022).

[20] Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, 2093/05/EN WP 114, at 14.

[21] PAUL VOIGT & AXEL VON DEM BUSSCHE, THE EU GENERAL DATA PROTECTION REGULATION (GDPR) A PRACTICAL GUIDE 131 (2017).

As to Article 5 (1) (1) of PCDF, it should also be understood as conferring the data processor Exemptions only when the transfer of personal information is necessary and occasional because: firstly, this rule uses “确需”, which has the same meaning of “necessary”; secondly, from a view of systematic interpretation, since Article 5 (1) (4) of PCDF deals with situations where transfers of personal information are not occasional but recurrent, Article 5 (1) (1) of PCDF should only deal with occasional transfers of personal information.

Besides, Article 5 (1) (1) of PCDF is only applicable where the data subject is the contract party, but not includes situations where the data subject is not the contract party. Instead, the contract is concluded between the personal information controller and the recipient in the interest of the data subject just as the formulation of Article 49 (1) (c) of GDPR. Justifications behind Article 49 (1) (b) and (c) of GDPR are similar,[22] it is relatively puzzling why PCDF only regulates situations where the data subject is the contract party, since the omission of situations in Article 49 (1) (c) of GDPR will immensely confines the scope of contract-based derogations, or, the Exemptions which ought to be treated equally as Article 5 (1) (1) of PCDF. For example, when there is an international bank transfer in the interest of the data subject, why the transferring party inside China cannot enjoy Exemptions under PCDF, while if the data subject is the contract party, who initiates the payment with a bank inside China, then the bank, as the data processor, can enjoy the Exemptions under PCDF. Since the data subject’s consent to the transfer of personal information does not exist in both cases, it is not convincing why different rules apply to similar situations. Besides, as to the cross-border delivery service, if the delivery company subcontracts the delivery work to the subcontractor for a better economic benefit out of division of labor theory, why the subcontractor who actually carries out the delivery and transfer the personal information cannot enjoy Exemptions, comparing to the delivery company executing the delivery itself? It is not persuasive why a subcontracting by the delivery company contracting with data subject will influence the Exemptions under PCDF.

Consequently, an expanding explanation of Article 5 (1) (1) of PCDF to include situations of Article 49 (1) (c) of GDPR, which allows Exemptions where the data subject as the beneficiary, should be preferred.

B. Exemptions for Cross-Border Human Resource Management

Article 5 (1) (2) of PCDF articulates that the data processor enjoys Exemptions if the personal information of any internal employee must be provided to an overseas recipient as needed for company’s human

[22] *Ibid.*

resource management requirement in accordance with relevant law and regulations. This situation can be regarded as a special situation of Article 5 (1) (1) of PCDF because the transfer of personal information is to perform the employment contract between the employee and the company. However, from a comparative view, this exemption situation is not recognized by GDPR, since the transfer happens not in occasional circumstances and not necessary for the performance. Guidelines from European Data Protection Board (EDPB) points out that a direct and object link between the performance of the employment and the transfer of personal information does not exist.[23] Also, the transfer of personal information inside the corporate groups is deemed as a transfer within a stable relationship where the transfer of personal information occurs systematically and repeatedly.[24]

Article 5 (1) (2) of PCDF takes evidently a different approach compared to GDPR, allowing the transfer of personal information in a stable relationship for the purpose of cross-border human resource management. This rule is a consonant of the Action Plan for Steadily Advancing High-level Opening up and Making Greater Efforts to Attract and Utilize Foreign Investment issued by PRC's State Council, which states that China will support data flow between foreign-funded enterprises and their headquarters to promote the safe and orderly cross-border transfer of research and development, production, sales and other data of foreign-funded enterprises.[25] Scholar also argues that justifications behind this rule is the trading logic of promoting cross-border business, reducing the cost of daily operation of transnational companies, since the complimentary duties of data outflow constitutes a burden for the enterprises having multinational business.[26] Except for the business operation requirement, it is noteworthy that transfer of personal information due to the need of cross-border human resource management normally only influences the rights of the employee, which is normally governed and protected by the employment contract and relevant labor laws and regulations, and does not involve the interest of state and societal interests. Consequently,

[23] EPDB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, at 8.

[24] *Id.*, at 9.

[25] Zhashi Tuijin Gaoshuiping Duiwai Kaifang Gengda Lidu Xiyin he Liyong Waizi Xingdong Fangan (扎实推进高水平对外开放更大力度吸引和利用外资行动方案) [Action Plan for Steadily Advancing High-level Opening up and Making Greater Efforts to Attract and Utilize Foreign Investment] (promulgated by the General Office of the State Council, Feb. 28, 2024, effective Feb. 28, 2024), General Office of the State Council (China).

[26] *See* Hong Yanqing (洪延青), *Zhongguo Shuju Chujing Anquan Guanli Zhidu de Zai Pingheng—-Jiyu Guojia jian Shuju Jingzheng Zhanlue de Shijiao* (中国数据出境安全管理制度的"再平衡"——基于国家间数据竞争战略的视角) [*"Re-balancing" China's Data Outbound Security Management System: A Perspective Based on Inter-National Data Competition Strategy*],
3 Zhongguo Falv Pinglun (中国法律评论) [China Law Review] 201, 208 (2004).

the necessity to supervise and regulate the transfer of personal information inside an enterprise may not exist.

When it comes to the application scope of Article 5 (1) (2) of PCDF, this rule is not confined to the conclusion of the employment contract and the enterprise's initial register of employee information, but also includes situations like employee insurance service, employee's vacation, employee's performance management and promotion, etc., where a transfer of personal information is required. As to the scope of employee, in the exposure draft of PCDF, only the personal information of internal employee (内部员工) is regulated by this rule, but in the final version, the PCDF does not confine the employee to those internal employees. A proper understanding may be that the employee refers to formal employee, thereby excluding the possibility of Exemptions of personal information of interns, job applicants, and family members of formal employees,[27] but the exact scope of employee still needs to be clarified by authorities.

C. Exemptions for Personal and Proprietary Safety in Emergency

To protect the life, health, or property safety of natural persons under emergent circumstances, the data processor can enjoy Exemptions when transferring the personal information to countries outside China according to Article 5 (1) (3) of PCDF.

A parallel stipulation can be found in Article 49 (1) (f) of GDPR, which states the transfer is initiated to "protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent."[28] Under the context of GDPR, the key prerequisite of this derogation rule is that the data subject is incapable of giving consent, including physical, mental and legal incapability, since the individual's consent is a critical and primary situation of derogation regulated by 49 (1) (a) of GDPR, to which 49 (1) (f) of GDPR functions as the exception. Therefore, when the data subject can give consent, 49 (1) (f) of GDPR is not applicable.[29] Besides, GDPR requires this derogation applies only when the medical treatment on the data subject or the protection or salvation of the data subject is necessary to save the data subject at stake.[30] Typical situations to which Article 49 (1) (f) of GDPR is applicable include

[27] *See* Huang Chunlin (黄春林) & Chai Mingyin (柴明银), Shuju Chujing zhi Kuajing Renli Ziyuan Guanli Huomian Guize de Lijie yu Shiyong (数据出境之"跨境人力资源管理"豁免规则的理解与适用) [Data Outflow: Understanding and Application of Exemptions rules on Cross-border Human Resource Management], Shuju Hegui (数据合规) [Data "Compliance"], Mar. 26, 2024, Website: https://mp.weixin.qq.com/s?__biz=MzU1MzAzNzcwNw==&mid=2247490165&idx=1&sn=b940f6a060359ca15d4dad8ac310910b&scene=21#wechat_redirect.

[28] GDPR, Article 49.

[29] EPDB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, at 13.

[30] CHRISTOPHER KUNER, LEE A. BYGRAVE & CHRISTOPHER DOCKSEY, THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 852 (2020).

medical treatment of an unconscious individual, and rescue operations in natural disasters like floods, hurricanes, earthquakes, etc.[31]

PCDF does not contain rules comparable to 49 (1) (a) of GDPR requiring the consent of data subject as the ground for derogation, so whether Article 5 (1) (3) of PCDF can follow a same interpretation pattern as 49 (1) (f) of GDPR remains in doubt. This Article maintains the following two opinions: firstly, a philosophical justification of Article 5 (1) (3) of PCDF is quite self-evident, considering that, the conditions, set by Article 38 of PIPL, that the processor must comply before the transfer of personal information, is stipulated to ensure the protection of personal interest and national security, in situations where personal lives or properties face an imminent threat, Exemptions are reasonable and can be inferred from the purpose of Article 38 of PIPL, since both rules are designed to protect personal interest, and the interests Article 5 (1) (3) of PCDF protects are in a more urgent situation and often in a higher hierarchy. Secondly, although PCDF does not signifies data subject's consent as a ground for Exemption, elaborations of 49 (1) (f) of GDPR can be referred to, since in many situations the data subject's consent is nowhere to find. The tricky situation only arises where the data subject is still conscious and capable of expressing the subject's own opinion about whether the subject prefers a transfer of personal information to protect his personal and proprietary rights, should the data processor still enjoy the Exemption? The answer should be no, because the transfer of personal information aims the protection of the data subject, and data subject's will should be respected, since the transfer of personal information may not be preferred, which can also imply that the situation is not emergent enough to constitute the Exemption rule of Article 5 (1) (3) of PCDF.

D. Exemptions for Transfer of Personal Information under Certain Quota

According to Article 5 (1) (4) of PCDF, if data processor other than a critical information infrastructure operator (hereinafter "CIIO") has transferred personal information which does not contain sensitive personal information of less than 100,000 individuals, then the data processor can enjoy Exemptions. Pursuant to Article 2 of Regulation on Protecting the Security of Critical Information Infrastructure, critical information infrastructure refers to any of the critical network facilities and information systems in important industries including public communication and information services, energy, transportation, water conservancy, finance, public services, e-government, and science, technology and industry for national defense, and any other that may

[31] EPDB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, at 13.

seriously endanger national security, national economy and people's livelihood, and public interests in the event that they are damaged or lose their functions or their data are leaked.[32] As a consequence, data processor falling outside the category of CIIO, whose daily business and situations where data transfer happens will normally not endanger the public interests, at least under certain quota.

Further question remains to be solved as to why the data processor transferring non-sensitive personal information under a quota of 100,000 pieces can enjoy Exemptions, considering the fact that transfer of personal information is still possible of causing great risks to the protection of rights of the data subjects. Article 5 (1) (4) of PCDF takes a totally different approach compared to Article 4 (1) (3) of Measures for the Standard Contract for the Outbound Transfer of Personal Information[33] (hereinafter "MSCO") taking effect in 2023, which requires data processor transferring personal information to overseas recipient conclude standard contract to protect the safety of the transfer of personal information, while Article 5 (1) (4) of PCDF loosens the requirement and de facto annuls Article 4 (1) (3) of MSCO, since according to Article 13 of PCDF, provisions in PCDF should prevail over any conflicts between PCDF and MSCO. Justification behind Article 5 (1) (4) of PCDF can only be based on China's positive attitude towards a more liberal transnational data free flow system, which China has highlighted in the Global Cross-border Data Flow Cooperation Initiative, advocating that "[governments] should support free data flows that do not violate national security, public interests, and personal privacy" and "regulatory measures do not constitute... the initiative, transfer of information which does not cause great risks to personal privacy should be tolerated to greater extent, and transfer of personal information which does not contain sensitive personal information generally will not cause danger to personal privacy, so the PCDF takes a positive attitude towards the free transfer of personal information without sensitive information.

IV. CONCLUSION

In conclusion, there is no doubt that the issuance of PCDF reflects China's resolution to pursue a more open, inclusive, equitable and safe global digital flow system, where an appropriate balance between the

[32] Guanjian Xinxi Jichu Sheshi Anquan Baohu Tiaoli (关键信息基础设施安全保护条例) [Regulation on Protecting the Security of Critical Information Infrastructure] (promulgated by the General Office of the State Council, Jul. 30, 2021, effective Sep. 1, 2021), GENERAL OFFICE OF THE STATE COUNCIL (China).

[33] *See* Geren Xinxi Chujing Biaozhun Hetong Banfa (个人信息出境标准合同办法) [The Measures for the Standard Contract for the Outbound Transfer of Personal Information] (promulgated by the Cyberspace Administration of China, Feb. 3, 2023, effective Jun. 1, 2023), CYBERSPACE ADMINISTRATION OF CHINA (China).

need of international trade and protection of national security and personal interests can be achieved. Exemptions rules concerning transfer of personal information can find justifications on different bases. Data processors operating data transit can enjoy Exemptions because of both the low risks of transit itself and the data classification and grading rules adopted by China. As to Exemptions for specific situations, rules stated in PCDF partly follow the formulation and principles in the derogation rule of GDPR, but partly transcend the relatively conservative attitude of GDPR on the protection of personal rights, and the transcend is illustrated in PCDF's not requiring an occasional and non-repetitive characteristic of transfer under certain circumstances based on a legislating inclination towards data free flow. It is worthed to be noted that certain Exemption situations like data subject's consent (Article 49 (1) (a)), or Exemptions for protecting public interest (Article 49 (1) (d)) are not acknowledged in PCDF, the practical importance of these situations needs to be considered by the legislator and further amendments or perfections of PCDF are highly anticipated.