The EU Non-Personal Data Free Flow Regime and Its Localization in China: Postprint

Authors: Zheng Linghan, Xiao Dongme

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

Abstract

[Purpose/Significance] Addressing the legal vacuum in China's digital economy development, this study explores normative experience from the EU's free flow regime for non-personal data. [Method/Process] Through web-based research methods, this paper systematically reviews non-personal data regimes in extraterritorial legal policies and employs inductive and deductive methods for deconstruction, concluding that the fundamental rationale underlying the EU's free flow regime for non-personal data lies in the inherent demands of the Digital Single Market strategy and the established institutional foundation for data free flow. [Results/Conclusion] The main components of the EU's free flow regime for non-personal data include abolishing data localization requirements, encouraging the formulation of self-regulatory codes of conduct for data portability, permitting competent authorities to access data for the performance of statutory duties, evaluating the implementation of the Regulation on the Free Flow of Non-Personal Data, and developing guidelines for its coordinated application with the General Data Protection Regulation, among other aspects. For China, it should incorporate the construction of an orderly flow regime for non-personal data into its legislative planning and establish rights to personal data portability and non-personal data migration in the drafting of the Personal Information Protection Law and the Data Security Law.

Full Text

Preamble

Vol. 63 No. 13 July 2019 ChinaXiv Cooperative Journal

EU Non-Personal Data Free Flow System and Its Localization in China

Zheng Linghan, Xiao Dongmei
Xiangtan University Law School, Xiangtan 411105

Abstract

[**Purpose/Significance**] Aiming at the absence of legal systems in China's digital economic development, this paper explores normative experience from the EU's non-personal data free flow system. [**Method/Process**] Using network investigation methods to sort out non-personal data systems in foreign legal policies, and employing inductive and deductive approaches for deconstruction, the study concludes that the fundamental reasons for the formation of the EU's non-personal data free flow system lie in the inherent demands of the Digital Single Market strategy and the established institutional foundation for data free flow. [**Result/Conclusion**] The main elements of the EU's non-personal data free flow system include abolishing data localization requirements, encouraging the development of self-regulatory codes of conduct for data porting, allowing authorized institutions to access data when performing official duties, evaluating the implementation of the Regulation on the Free Flow of Non-Personal Data (RFFND), and developing guidance on its coordinated application with the General Data Protection Regulation (GDPR). For China, the construction of an orderly flow rule system for non-personal data should be included in legislative planning, with rights to personal information portability and non-personal data migration established in the drafting of the Personal Information Protection Law and the Data Security Law.

From the agricultural revolution and industrial revolution to the information revolution and today's digital revolution, each major technological innovation has ushered society into a new economic era. The social transformation brought by digital technology has unleashed the growth potential of the digital economy, making data a new resource and production factor. The sustainable development of the digital economy depends on both data protection and utilization, making the construction of rules for data protection and free flow a fundamental issue for sustainable data economy development. The EU resolved legal obstacles for unified data protection rules across member states through the General Data Protection Regulation (GDPR). Simultaneously, the EU has taken the lead in constructing a system for personal data free flow: on one hand, with GDPR as the hallmark, it has formed a legal rule system for personal data protection and free flow; on the other hand, represented by the Regulation on the Free Flow of Non-Personal Data (RFFND), it has formed a legal system for non-personal data free flow. The free flow of personal and non-personal data constitutes the entirety of data flow. In its process of forming a digital integrated market, the EU has built a data free flow institutional system, while China is still in the "eve" of establishing specialized systems for data protection and utilization. Compared with GDPR, which took effect in May 2018, RFFND also has practical significance for research.

Currently, domestic research on GDPR interpretation, analysis, and its impact on university library work is abundant, but substantive research on RFFND is extremely scarce. Meanwhile, Article 69 of China's current E-Commerce Law has already declaratively emphasized the orderly free flow of e-commerce data

in accordance with law and that the state should take measures to promote the establishment of a public data sharing mechanism. In view of this, it is necessary to examine the social background behind RFFND, focus on analyzing the non-personal data free flow system, and extract its implications for China's digital economic development, in order to provide references for the sustainable prosperity of China's digital economy.

1 Formation of the EU's Non-Personal Data Free Flow System

In the first wave of digitalization, American internet technology companies represented by Google have already occupied the EU market, and the EU has lost its first-mover advantage in emerging technology fields such as the internet, cloud computing, big data, and artificial intelligence. Entering the digital economy era, the EU attempts to ensure its leading global position in the digital economy by achieving the strategic goal of a digital single market, thereby shifting to building corresponding digital economic order institutions to gain first-mover advantages and respond to technological challenges and economic pressures from American high-tech companies. Therefore, when deconstructing the EU's non-personal data free flow system, attention should be paid to its digital single market strategic demands and its established institutional foundation for personal data free flow.

1.1 Inherent Reason: Inherent Demand of the EU's Digital Single Market Strategy

In the 2018 Global Digital Economy Development Index ranking of 150 countries, the United States, China, and the United Kingdom ranked top three with indices of 0.837, 0.718, and 0.694 respectively, while the average index for the 28 EU member states (still including the United Kingdom) was 0.4855, ranking 22nd. The EU's 2018 Digital Economy and Society Index (DESI) Report comprehensively compares the digital economy and social development of EU member states relative to 17 non-EU countries from five dimensions or policy areas: broadband connectivity, human capital (digital skills), internet application, digital technology integration, and digital public services. The report depicts the digital competitiveness development level of the entire EU and its member states, with the 28 EU countries averaging 54.0 points, Denmark ranking first, and Romania, Greece, and Bulgaria scoring the lowest, with significant gaps remaining between the best and worst performers. From both the overall EU ranking and differences among member states, the EU digital single market remains to be perfected, indicating possible obstacles in technology and law for data-driven economic development. Due to the objective existence of member states' own digital technology disadvantages, the impact of data flow restrictions on new technology development and application is amplified. A rule framework for non-personal data free flow urgently needs to be established, as data localization requirements have been identified as a major obstacle affecting

data sharing.

The EU Commission's mid-term review report on the Digital Single Market Strategy, based on assessing progress made, calls on co-legislators to act swiftly on all submitted proposals and outlines further actions regarding online platforms, digital economy, and cybersecurity. According to the mid-term review report, the EU Commission is working to solve the accessibility and reusability issues of public data and personal data with public interest attributes. The legal proposal for an EU data free flow cooperation framework was put forward, meaning the EU recognizes the differences between non-personal and personal data in terms of privacy protection, economic value, and social impact, and focuses on establishing a rule order for non-personal data flow different from personal data protection and flow systems.

In fact, the EU's Digital Single Market Strategy had already proposed eight major legislative recommendations, including coordinating digital rights. From the roadmap for completing the digital single market, both GDPR and RFFND represent the EU's step-by-step actions in "data ownership, data free flow (such as between cloud service providers), and European cloud." After GDPR took effect, the EU could apply unified rules to protect personal data. The regulation prevents restrictions on personal data free flow within the EU, yet member states might restrict non-personal data free flow for other reasons (not for personal data protection). Additionally, issues regarding ownership, operability, usability, and data access of newly emerging machine-generated data (non-personal data) also need to be resolved. In summary, because the EU lacks advantages in digital technology leading to lagging digital economy, the EU attempts to build relevant data institutions to find breakthroughs and boost its digital economy development through institutions.

1.2 External Reason: Institutional Foundation for EU Data Free Flow Already Established

First, personal data free flow rules. After GDPR was introduced to China, more research focused on its purpose of protecting personal data while neglecting GDPR's other purpose of promoting personal data free flow within the EU. On one hand, Article 1 of GDPR stipulates that the protection of natural persons regarding personal data processing cannot restrict or prohibit personal data free flow within the EU, actually determining the necessary limits of personal data protection. On the other hand, Article 20 of GDPR establishes the right to data portability, thereby empowering individuals' control over data and providing space and operational possibility for personal data free flow to a large extent. Because exercising this right involves transferring personal data from one data controller to another, as a regulation directly applicable to EU member states, GDPR has laid the foundation for personal data free flow in the EU.

Second, non-personal machine-generated data free flow rules. In the Communication on Building a European Data Economy, the EU Commission intends to

unleash the reuse potential of different data types and their cross-border free flow to achieve the European digital single market, proposing to encourage (and in special cases mandate) companies to grant third parties access to their data to promote data exchange and value addition through "data producer rights." Data utilization and reuse cannot be separated from data free flow. The prerequisite for allowing data to flow freely in the market is clear data ownership. Regardless of which subject the rights are initially allocated to, as long as the ownership is clear, market mechanisms can promote data free flow. Data producer rights refer to the rights of "owners or long-term users" of sensor devices, aiming to give data producers more choices through these rights, helping them use data and unlock machine-generated data held by manufacturers. By establishing data producer rights, non-personal or anonymized machine-generated data can be maximally promoted, thereby truly establishing an order framework for non-personal data free flow. Although data producer rights have not yet been formally established as a statutory right, they have been proposed in the communication and extensively discussed by various parties, laying the foundation for establishing a free flow order for non-personal data.

In summary, data free flow encompasses both personal and non-personal data free flow. The EU has already formed personal data free flow rules and prepared for establishing non-personal machine-generated data free flow rules. Therefore, establishing a non-personal data free flow system is a logical next step.

2 Main Content of the EU's Non-Personal Data Free Flow System

In November 2018, RFFND [(EU) 2018/1807] officially completed the EU legislative process. The regulation took effect on the twentieth day after its publication in the Official Journal of the EU, became applicable six months after publication, and is directly applicable to all member states. The regulation aims to establish rules on data localization requirements, provision of data to authorized institutions, and data porting by professional users, thereby forming a framework for non-personal data free flow and ensuring non-personal data free flow within the EU.

2.1 Abolition of Data Localization Requirements

In RFFND, "data localization requirement" refers to any obligation, prohibition, condition, restriction, or other requirement in member states' laws, regulations, or administrative provisions, or resulting from general and continuous administrative actions implemented by member states and bodies governed by public law (including in public procurement), that forces data processing to be conducted within a specific member state or hinders data processing in any other member state, without affecting the implementation of Directive 2014/24/EU (on public procurement and repealing Directive 2004/18/EC). The most basic requirement of the EU's non-personal data free flow system is the abolition of

data localization requirements, with only "public security purposes and compliance with the principle of proportionality" as exceptions. Therefore, EU member states should modify existing data localization requirements according to the procedures stipulated in Articles 5, 6, and 7 of EU Directive 2015/1535 (establishing procedures for information in the field of technical regulations and rules on Information Society services), or immediately report any draft law introducing new data localization requirements to the EU Commission.

By May 30, 2021, member states should ensure that provisions in their current general laws, regulations, or administrative provisions violating Article 4(1) of the regulation are repealed. If a member state believes that measures involving data localization requirements do not violate the regulation's data localization requirements, it should report to and explain the reasons to the EU Commission. Without prejudice to Article 258 of the Treaty on the Functioning of the European Union, the EU Commission should review whether the measures comply with Article 4(1) of RFFND within six months of receiving the member state's report and, where appropriate, propose opinions or suggest modifications or repeal of the measures to the member state concerned.

Member states should disclose all specific circumstances of data localization requirements in their current national laws, regulations, or administrative provisions through an independent national online information channel and update them in real time, or establish a unified information disclosure channel across the EU to disclose all such latest data localization requirements according to another EU legal provision, and report the address of the online information channel to the EU Commission. The EU Commission should publish links to such addresses on its website and regularly update a comprehensive list and summary information of current domestic data localization requirements reported by member states.

2.2 Professional User Data Porting

In RFFND, "service provider" refers to a natural or legal person providing data processing services; "user" refers to a natural or legal person using or requesting data processing services, including public institutions or bodies governed by public law; "professional user" refers to a natural or legal person using or requesting data processing services for purposes related to their trade, business, craft, professional service, or task, including public institutions or bodies governed by public law. The EU Commission should encourage and facilitate the development of self-regulatory codes of conduct uniformly applicable to EU member states to further build a competitive data economy based on transparency, interoperability, and open standards, mainly from four aspects:

First, best practices to facilitate changing service providers or porting data in structured, commonly used, and machine-readable formats (including open standard formats requested or required by the receiving service provider). Second, minimum information requirements to ensure that when professional users in-

tend to change to another service provider or port data to their own IT systems before the expiration of data processing contracts, they can obtain sufficiently detailed, clear, and transparent information regarding data processing, technical requirements, timing, and charges. Third, certification schemes to establish programs that help professional users compare data processing products and services (including quality management, information security management, business continuity management, and environmental management), while considering existing national or international norms to enhance the comparability of such products and services. Fourth, communication approaches using multidisciplinary methods to raise stakeholder awareness of self-regulatory codes of conduct.

The EU Commission should work closely with all stakeholders, including SMEs, start-up associations, users, and cloud service providers, to develop self-regulatory codes of conduct, and should urge service providers to complete the development of such codes by November 29, 2019, and implement them effectively by May 29, 2020.

2.3 Authorized Institution Access to Data

In RFFND, "authorized institution" refers to a national authority of a member state or other body authorized by national law to perform public functions or exercise official powers that has the right to access data processed by natural or legal persons when performing official duties under EU or member state law. This regulation does not affect the power of authorized institutions to request, obtain, or access data when performing official duties under EU law or member state law, and cannot refuse authorized institution access to data on the grounds that the data is processed in another member state.

When an authorized institution requests access to user data but fails to obtain it, and there is no specific cooperation mechanism for data exchange between authorized institutions of different member states under EU law or international agreements, the authorized institution may request assistance from another member state's authorized institution according to the procedure stipulated in Article 7 of RFFND. If the assistance request necessarily requires the requested party to access any facilities of natural or legal persons (including any data processing equipment and tools), such access must comply with EU law or national procedural law. Member states may impose substantive, appropriate, and deterrent penalties for failure to fulfill data provision obligations in accordance with EU law and domestic law.

In cases of user power abuse, member states may, when necessary and according to the urgency of data acquisition while considering the interests of relevant parties, strictly adopt temporary measures complying with the principle of proportionality against the user. If temporary measures require data relocalization lasting more than 180 days, the member state should inform the EU Commission of such temporary measures within 180 days. The EU Commission should

review the temporary measures and their compliance with EU law as soon as possible and take necessary measures where appropriate. The EU Commission should exchange information on experience gained in these aspects with the single contact points of member states designated under Article 7 of RFFND.

2.4 Inter-Agency Cooperation Procedures

Each member state should designate a single contact point for communication with other member states and the EU regarding the application of RFFND, and should report the designated independent contact point and subsequent changes to the EU Commission. The single contact point should provide users with general information about RFFND, including self-regulatory codes of conduct.

If an authorized institution of a member state requests assistance from another member state to obtain data according to Article 5(2) of RFFND, it should submit a justified request to the single contact point designated by the other member state. The request should include a written explanation of reasons and the legal basis for accessing data. The single contact point should identify the relevant authorized institution of the member state and forward the request to that institution. The authorized institution receiving the forwarded request from the single contact point should not unduly delay and should respond within a timeframe appropriate to the urgency of the request regarding whether to grant data access, or inform the requesting member state's authorized institution that the request does not meet the conditions for assistance under RFFND.

According to Article 5(2) of RFFND, any information exchanged in requested and provided assistance can only be used for the requested matter.

2.5 Implementation Evaluation and Guidance

The EU Commission should, by November 29, 2022, submit an implementation report on RFFND to the European Parliament, the Council, and the European Economic and Social Committee, mainly including three aspects: first, the application of RFFND, particularly regarding datasets composed of personal and non-personal data, considering the possibility of re-identifying anonymized data with market and technological development; second, member states' implementation of Article 4(1) of RFFND, particularly concerning public security exceptions; third, the development and effective implementation of self-regulatory codes of conduct and the provision of effective information by service providers.

Member states should provide the EU Commission with necessary information for compiling the RFFND implementation report. By May 29, 2019, the EU Commission should publish guidance on the coordinated application of RFFND and Regulation (EU) 2016/679 (GDPR), particularly regarding datasets composed of personal and non-personal data.

3 Localization of the Non-Personal Data Free Flow System in China

The EU focuses on eliminating technical and legal obstacles in its digital economic development by enacting laws and regulations directly applicable to member states, thereby removing major legal obstacles. For example, GDPR and RFFND also contain provisions on unified technical standards, which help eliminate technical obstacles to some extent. A set of universal and certain legal rules in member states is a key factor for all market entities to participate in internal market competition. RFFND is the EU's first regulation establishing unified rules for non-personal data after GDPR addressed personal data, forming an institutional framework for EU non-personal data free flow and further perfecting the data free flow rule system. In China, the Political Bureau of the CPC Central Committee conducted its second collective study on implementing the national big data strategy, where Xi Jinping emphasized the need to establish systems for data resource 确权 (rights confirmation), opening, circulation, and trading, improve the data property rights protection system, strengthen research on international data governance policy reserves and governance rules, and propose China's solutions [15]. By analyzing the main content of the EU's non-personal data free flow system, we can obtain implications for China's data resource rights confirmation, opening, circulation, and trading institution construction.

3.1 Constructing an Orderly Flow Rule System for Non-Personal Data

Currently, China has not yet issued specialized personal data protection rule systems, let alone specialized non-personal data free flow rule systems. From the series of specialized local regulations and national standards on big data or data that have been released or are being formulated (see Table 1), data flow (trading) has begun to receive attention, but the overall focus remains on data security. Additionally, the Data Security Law has been included in the first category of legislative projects of the 13th National People's Congress Standing Committee, representing legally mature drafts to be submitted for deliberation within the term [16]. This indicates that future specialized legislation on data protection will also focus on "data security." However, from the perspective of global digital economic development trends, data flow is fundamental for reducing enterprises' economic burden of using data, developing the digital economy, enhancing innovation capacity, and strengthening social production competitiveness. It is necessary to promote and regulate non-personal data free flow and its processing activities by forming universal and stable data free flow legal systems domestically or regionally.

Under the current trend of China 致力于 (working on) the "Data Security Law" institutional construction, this opportunity should be used to embed non-personal data free flow rules into the legislation by setting up relevant chapters on "Non-Personal Data Free Flow Security." Without violating China's data localization storage requirements, personal and non-personal data should be distinguished

to strengthen the construction of data free flow rule systems. This is feasible under the current legal framework because at the civil law level, China's current General Principles of Civil Law Articles 111 and 127 establish a "dual" protection model for personal information and data. Personal data can be absorbed into China's existing personal information legal protection framework—the terms "personal data" and "personal information" are different legal terminology choices for the same object, with value judgments pointing to almost identical objects.

Moreover, the rule construction for non-personal data free flow should also focus on government data (public data). Currently in China, not only has data between government departments (public sectors) not been fully connected, but also open sharing of government affairs data (public data) has not been truly realized. There are no relevant legal norms to guide and promote this, and the government's motivation to promote data opening is not strong.

3.2 Establishing Rights to Personal Information Portability and Non-Personal Data Migration

Article 20 of GDPR grants data subjects the right to data portability. If a data subject has provided personal data related to them to a data controller, they have the right to obtain such data in structured, commonly used, and machine-readable format from the data controller, and the data controller cannot hinder the data subject from transferring these data to another data controller. The right to data portability not only enhances individuals' ability to control their data but also provides rebalancing of the relationship between data subjects and data controllers, objectively helping to activate competition in the online service market. Furthermore, Article 6 of RFFND sets forth "data porting" provisions, but unlike using "shall assist" or "shall not hinder" data porting to grant professional users the right to data migration, it "encourages and facilitates" the development of self-regulatory codes of conduct uniformly applicable to EU member states, while requiring the EU Commission to treat users as stakeholders in close cooperation when developing such codes. Therefore, this provision cannot be understood as establishing a "right to data migration." The right to personal data portability and self-regulatory codes of conduct for non-personal data migration have become guarantees for private entities to participate in data (both personal and non-personal) free flow. In terms of substantive content: the right to data portability tends to ensure that data subjects (ordinary individuals) can change service providers, such as requiring Alipay to transfer payment data to Tencent Wallet; self-regulatory codes of conduct for data migration focus more on ensuring that data users (mainly professional users) can use or process data, such as requiring the JD.com platform to import merchant customer data into specific analysis platforms for subsequent precision marketing.

Data free flow includes both personal and non-personal data utilization: on one hand, personal data is the core data resource for current business operations. Personal data must be effectively protected and should also be allowed to flow

freely, meaning data subjects can trade their personal data to other subjects under their effective control. On the other hand, non-personal data already exists in large volumes in modern industrial and agricultural automation production fields, especially with the continuous development of new technologies such as the Internet of Things, artificial intelligence, and machine learning. The volume and utilization demand of non-personal data will continue to grow. As long as non-personal data free flow within China does not involve high-level values such as personal privacy or information, trade secrets, or national security, it should be fully utilized. More importantly, an effective mechanism for converting personal data to non-personal data should be established. While focusing on protecting personal information security, strengthening non-personal data free flow will help achieve internal market balance between personal information protection and data utilization (including personal data utilization).

The demand for data portability or migration should be addressed in China's future legislation. Whether personal or non-personal data, it should be made portable or migratable to promote service providers to improve service quality through competition and enhance total consumer welfare. According to China's General Principles of Civil Law, which establishes a dual structure for personal information and data, and considering that the Personal Information Protection Law and Data Security Law are listed as specialized laws in the first category of legislative projects of the 13th National People's Congress Standing Committee [16], rights to data portability and data migration can be arranged in future legislation in accordance with China's legal culture and legislative techniques: first, establish principle or guiding provisions for personal information portability rights under the "personal information" chapter of the Personality Rights section of the Civil Code, and set specific personal information portability right provisions in the formulation of the Personal Information Protection Law; second, directly specify non-personal data migration provisions under the relevant chapter on "Non-Personal Data Free Flow Security" in the Data Security Law.

GDPR's 99 articles forming a personal data protection and free flow rule system have created a global demonstration effect: on one hand, since GDPR officially took effect on May 25, 2018, California has introduced the California Consumer Privacy Act, India has officially released the Personal Data Protection Bill, and Brazil has officially approved the General Data Protection Bill submitted by the Senate; on the other hand, American internet giants such as AT&T, Amazon, Google, Twitter, and Apple have called on the US to follow the EU GDPR example by enacting unified data privacy protection laws at the federal level to avoid the California Consumer Privacy Act creating a legislative demonstration effect in other states, causing technology companies to follow different rules in different states and increasing compliance costs. As a supplement to GDPR, although RFFND contains only nine articles, it forms a differentiated data protection and data flow legal system framework with GDPR in the EU, collaboratively stimulating data economic value, and may also create legal demonstration effects in countries and regions that have already issued or will soon issue specialized data protection laws.

Currently, China's digital economy construction legal system is not yet sound, mainly relying on national-level policies such as the "Big Data Development Action Outline" and "Big Data Industry Development Plan (2016-2020)," as well as local big data industry policies issued by Guizhou, Guangdong, Zhejiang, Fujian, and other provinces to promote digital economy construction. However, China's digital transformation expenditure market size will increase from 2.8 trillion yuan in 2019 to 3.7 trillion yuan in 2021 [17], meaning China's digital economy scale continues to expand. Consequently, market demand for data free flow will also grow stronger. Whether national law can properly coordinate personal information protection and non-personal data orderly flow will become a key factor for sustainable digital economy development. Abolishing data localization, professional user data porting, authorized institution data access, inter-agency cooperation procedures, and implementation evaluation guidance constitute the core content of the non-personal data free flow system. For China's current data rule of law soil: on one hand, an orderly flow rule system for non-personal data should be constructed from top-level design based on the above core content; on the other hand, the approach of granting professional users migration rights should not be copied. Instead, combining China's General Principles of Civil Law Articles 111 and 127 forming the "personal information" and "data" dual protection structure, rights to personal information portability and non-personal data migration should be established.

References

[1] EUR-Lex. 32018R1807. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance) [EB/OL]. [2018-12-05]. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1546391029521&uri=CELEX:32018R1807.

[2] Huang Guobin, Zhang Shasha, Yan Xin. Research on the concept and basic types of personal data [J]. Library and Information Service, 2017, 61(5): 41-49.

[3] Greafi, Gellert R, Purtova N, et al. Feedback to the commission's proposal on a framework for the free flow of non-personal data [EB/OL]. [2019-02-27]. https://ssrn.com/abstract=3106791.

[4] He Yuyan. Interpretation of EU General Data Protection Regulation and its implications for personal data protection in China [J]. Library and Information Science Tribune, 2018, 3(11): 67-72.

[5] Tian Xinyue. Analysis of new rules in EU General Data Protection Regulation [J]. Wuhan University International Law Review, 2016, 19(2): 466-479.

[6] Li Ping, Zhou Lihong, Ying Minglei. Analysis of EU General Data Protection Regulation and its impact on university library work [J]. Library Science Research, 2018(20): 35-41, 54.

[7] Ali Research Institute, KPMG. 2018 Global Digital Economy Development

Index Report [EB/OL]. [2019-02-28]. http://www.cbdio.com/BigData/2018-09/20/content_{5842460}.htm.

[8] Digital single market. International digital economy and society index 2018 [EB/OL]. [2018-12-05]. https://ec.europa.eu/digital-single-market/en/news/international-digital-economy-and-society-index-2018.

[9] Digital single market. Digital single market mid-term review [EB/OL]. [2018-12-05]. https://ec.europa.eu/digital-single-market/en/news/digital-single-market-mid-term-review.

[10] Digital single market. Shaping the digital single market [EB/OL]. [2018-12-05]. https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market.

[11] EUR-Lex. 52015DC0192. A digital single market strategy for Europe [EB/OL]. [2018-12-05]. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A192%3AFI

[12] Digital single market. Building a European data economy [EB/OL]. [2018-12-30]. https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy.

[13] Cao Jianfeng, Zhu Linhua. Preliminary exploration of European data property rights [J]. Information Security and Communications Privacy, 2018(7): 30-38.

[14] Jowefd, Reto M, Jure G, et al. Public consultation on building the EU data economy [EB/OL]. [2018-03-25]. https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_{{{

[15] Xinhua News Agency. Xi Jinping presides over the second collective study of the Political Bureau of the CPC Central Committee [EB/OL]. [2018-12-09]. http://www.gov.cn/xinwen/2017-12/09/content_{5245520}.htm.

[16] NPC. 13th National People's Congress Standing Committee legislative plan [EB/OL]. [2018-12-31]. http://www.npc.gov.cn/npc/xinwen/2018-09/10/content_{2061041}.htm.

[17] CCID Digital Transformation White Paper [EB/OL]. [2019-04-28]. http://www.cbdio.com/BigData/2019-01/08/content_{5980314}.htm.

Author Contributions: Zheng Linghan: Collected and organized materials and wrote the full text; Xiao Dongmei: Guided revisions and reviewed the paper.

Zheng Linghan, Xiao Dongmei. The Free Flow of Non-Personal Data in EU and its Localization in China [J]. Library and Information Service, 2019, 63(13): 122-128.

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