European Union Law on the Digital Single Market:

The Legal Issues of Transborder Data Flows

on Personal Information

By

WU YANG (M-B7-5085-6)

Master of Law in European Union Law

2020

Faculty of Law

University of Macau

European Union Law on the Digital Single Market:
The Legal Issues of Transborder Data Flows
on Personal Information

by

WU YANG

SUPERVISOR: Prof. Paulo Canelas de Castro

Master of Law in European Union Law

2020

Faculty of Law

University of Macau

Abstract

Nowadays, numerous personal data transfer cross-border and flowing in the digital world, the personal data not only the valuable resources of the multinational corporations but also has become one of the fundamental driving forces of globalization and the global digital economy. Meanwhile, the transborder data flow also means the administration and supervision on the personal data and information are complicated and troublesome especially in the digital world and the personal data subjects too hard to seek the remedies and redress when their rights have been infringement. And different countries' legislation of personal data protection naturally exists gaps in the implementation and enforcement, which also brings challenges for the corporations to collect, use, control, and process the data. Therefore, this thesis trying to analysis the EU's legal framework of personal data protection in the transborder data flow.

The first chapter is an introduction of the Digital Single Market strategy (DSM) of the EU, figures out the objectives of the DSM strategy and explains the what kind of roles that data protection takes into place in the DSM Strategy, and why the data security is such important to the EU digital economy. Then, introduce the definition of the transborder data flow and its relations with the data security, how the transborder data flow influences the digital economy, personal daily life, and even the public interest and national security.

The second chapter could be divided into two parts. One part will come from the perspective of the historical development of personal data protection to analyse EU laws. From the "Hessisches Datenschutzgesetz" to the "Convention for the Protection of Individuals concerning Automatic Processing of Personal Data (Convention 108)", and to the "Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Directive)", this directive is the most important legislation on the personal information protection in transborder data flow at an early age in the EU, it forms the fundamental mechanism on the personal data protection and the general approaches for the cross-border data transfer, the adequate level of protection, the Binding Corporate Rules, the Standard Contractual Clauses was

designed by the Directive. And also introduce the EU and U.S. bilateral agreement on data transfer, the Safe Harbor Framework, and how it collapsed. The other part is the specific analysis of the "General Data Protection Regulation", the GDPR take into force embodied the EU's personal data protection framework took a step forward into a new stage. The GDPR not only extended the jurisdiction scope formed the long-arm jurisdiction but also amplified the data subject's rights, added the data portability right and the erasure right. Moreover, the supervision mechanism and the rules of legal redress and penalties also has been improved. And this part also mentioned the Privacy Shield Framework, which replaced the Safe Harbor Framework.

The third chapter is mainly about the comparison of the EU transborder data flow regulations with other countries and international organisation, mainly compared with the U.S., China, and APEC. The attitude and the trends of the U.S. in personal data protection are different from the EU, the EU's policies based on the protection of human rights and the U.S.'s policies based on the commercial interest. Therefore, the U.S. approaches of the transborder data flow rely on industrial self-discipline and international agreements. And the APEC also established the Cross-Border Privacy Enforcement Arrangement (CBPA) and Cross-Border Privacy Rules (CBPR) which leading by the U.S., the core principle of CBPR is similar to the U.S. approach. The Chinese legal framework of the personal information protection still at the initial stage, the rules are separated in different industrial guidelines, national standard, and departmental directives, and the approaches of the personal information transfer cross-border also limited.

The conclusion contains several opinions and suggestions for the further reforms on the legislation of the personal data transfer cross-border. First, the proposal of the personal data classification and hierarchy system, combined with the reforms on the consent clauses to improve the defects of companies' privacy policies in practice. Second, adjust the EU's policies on the data localization to remove the obstacles and hinders of the data flows, make the regulations and laws more realistic and flexible for implementation. Third, the EU should take active actions to form a general world digital trade agreement and multilateral cooperation framework and pursue the leading position in the global transborder data flow governance system.

Keywords

Personal Information Protection; Transborder Data Flow; Digital Single Market; Digital Economy; GDPR;

Declaration

I declare that the thesis here submitted is original except for the source materials explicitly acknowledged and that this thesis as a whole, or any part of this thesis has not been previously submitted for the same degree or for a different degree.

I also acknowledge that I have read and understood the Rules on Handling Student Academic Dishonesty and the Regulations of the Student Discipline of the University of Macau.

21/08/2020

Abbreviations

APEC	Asia-Pacific Economic Cooperation
BCRs	Binding Corporate Rules
CAC	Cyberspace Administration of China
CPEA	Cross Border Privacy Enforcement Arrangement
CBPR	Cross-Border Privacy Rules
CLOUD	Clarifying Lawful Overseas Use of Data Act
DPA	Data Protection Authority
DPD	Data Protection Directive (the Directive)
DSM	Digital Single Market
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ECJ	European Court of Justice
ECPA	Electronic Communications Privacy Act
EDPB	European Data Protection Board
EU	European Union
FTC	United States Federal Trade Commission
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GPEN	Global Privacy Enforcement Network
ICT	Information and Communications Technology
ISP	Internet Service Provider

JOP	Joint Oversight Panel
NSA	United States National Security Agency
OPA	Online Privacy Alliance
RFPA	Right to Financial Privacy Act
SAC	Standardization Administration of China
SMEs	Small and Medium-Sized Enterprises
SCC	Standard Contractual Clauses
US	United States
VAT	Value Added Tax
WTO	World Trade Organisation

Introduction

1. Research Background

Nowadays, with the development of the Information and Communication Technology, more and more new technologies are emerging and deeply changer our daily life, like the Bigdata, the Artificial Intelligence, the Cloud Computing, and the BlockChain. Meanwhile, the personal data transfer cross-border are easier then old-days and become a common phenomenon, especially when our life highly rely on the internet. Meanwhile, the data also have uncountable value for the corporations on the business, especially for those multinational internet enterprises, the data itself also could be treated as the goods on the international digital trade. Undoubtedly, data plays a vital role in the digital world economy. However, the data also will face unpredictable risks when it transfers cross-border, and the data security problems will be a tough nut to crack when those data contained personal information.

The personal data also connect with personal privacy, once the data security incidents happened, and personal data was leaked, the fundamental human rights might be an infringement, and the individual's property may suffer loss. Moreover, some critical personal information even could influence the public interest and national security, hence, the protection of the personal data cross-border flow has become an eye-brow burning issue in the world. The first EU legal instrument of the personal information protection is the "*The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108)*" which published in 1985, then, in 1995, the first comprehensive EU directive of the data protection has been published, the "*Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (the Directive)* ", the Directive established the fundamental legal framework of the personal data protection. Also, it contained the rules about the personal data cross-border flow. And with the time passing, the "*General Data Protection Regulation*" was into the force in 2018 under the situation that the EU announced to establish the "Digital Single Market".

The cross-border flow of information and data is an inevitable trend in the development of the era of big data, and it is incompatible with the pattern of the development to prohibit the cross-border transfer of personal data.

However, the protection of personal information involves the fundamental rights of citizens and should not be ignored. The EU and other countries or organisations are pursuing to find a perfect balance between the personal privacy protection and the free flow of the data, hence, this thesis trying to analysis the EU laws of the transborder data flow and compare with the laws, regulations, or international agreements, in the U.S., China, and the APEC, then bring out the several opinions and suggestions for the further reforms on the legislation of the personal data transfer cross-border.

2. Research Questions

The primary purpose of the dissertation is from the departure point of describing and grasping characters of Transborder Data Flows, analysis law and policies like the leader states and a dynamic region. Then, figuring out suitable solutions for the EU and other states. By summarizing and evaluating those activities of regulation, we would analyse the tendency of Transborder Data Flows policies and regulations in the EU. Meanwhile, we would try to compare and analyse the other regions' experience, try to absorb the advanced measures in other leader states to keep those solutions also suitable for the future.

The thesis mainly encircles the following questions to proceed:

a) What is the best solution for the EU to promote the digital economy?

b) What are the problems of the modern legal framework on the transborder data flow?

c) How to find an excellent balance between the personal data protection and data free flows?

3. Methodology

The main methods used to write the thesis are both induction and deduction on the premise of historical researches, and it is necessary to set off the research from the angle of history, then we can find out the achievements we have finished, the situation we are facing and the objects that will be set for the next stage in a long and a short period. Besides, the comparative method can be useful when talking about similar Transborder Data Flows policy in other regions, since that, the comparison and groping for a better solution to protect the essential data when it cross-border flow is a practical way to research. By research from the document and literature also summary of another excellent thesis, then achieve the goals step by step. If

possible, I will try to find the relevant case to analyze the application of specific policies and laws individually.

The way to fetch the research materials are libraries resources and library's online databases; journal indexes; official website indexes; current affairs reporting and newspapers etc. The different kinds of materials quoted and analyzed in the dissertation mainly come from the following sources:

Primary sources:

(a) Official documents of EU; U.S.; CHINA and APEC or other organizations.;

(b) Treaties, EU legislation, directives, regulations, and communications;

(c) Policy statements.

Secondary sources:

(a) Academic works of other scholars online

(b) The comments and papers in the journals.

1. Chapter One: The Relationship between the Digital Single Market and Data Protection

1.1. Introduction of the Digital Single Market

1.1.1. What is the Digital Single Market?

On the 15 July 2014, Jean-Claude Juncker, the Candidate president of the European Commission at that time, made a famous speech "*A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change*" at Strasbourg. In this speech, the notion of Digital Single Market has been officially coming out for the first time. Then, in May 2015, the Juncker Commission formally published the "*A Digital Single Market Strategy for Europe*".[1] You could easily smell the great ambitions of the European Union to establish the Digital Single Market, several high-level and long-term objectives has lain down on this document. In general, the DSM strategy will be built on three pillars. First one is aimed to create a better digital commercial atmosphere for the consumers and businesses; the second one is aimed to flourish the circumstances of digital networks and services, the third pillar is aimed to stimulate the potential digital economy of European Union.

The Digital Single Market is part of the Digital Agenda for Europe 2020 program of the EU, an initiative of Europe 2020 proposed strategy and it is the crucial content of the Single Market of the European Union.[2] The ultimate objectives of the Single Market are to achieve the four free-movements on persons, goods, service and capital in the internal market at the EU level, the trends of Internet Technology highly developed made the free-movement of information not just became the vital element of economic growth but also made the internet provide the new highway for the new goods and resources. The investment of Internet Technology will reflect on the growth of GDP has become a common view of the global market, based on the economic analysis of past three decades, a US $1 investment in digital technology will trigger a US $20 rise in GDP at

[1] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A Digital Single Marker Strategy for Europe*, COM(2015) 192 final, 6 May 2015, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015DC0192 .
[2] European Commission, "Europe 2020 strategy," available at: https://ec.europa.eu/digital-single-market/en/europe-2020-strategy .

a global level. The average return to GDP at investment in digital technology area is 6.7 times higher than non-digital investment.[3] Undoubtedly, we are already coming into a new revolutionary era raised by digital technology, then the EU finally conscious of the strategic status of ICTs in the battle of the world-leading position in the digital economy.

Nowadays, the tremendous digital resources flowing on the internet at the international level are pushing the innovation and development of communication technology and internet services. According to the report of McKinsey & Company,[4] Digital Network Industry nearly added $2.8 trillion to world GDP in 2015, exceeding the impact of the global goods trade. The traditionally transnational commerce and investment industry's contributions to global economic growth have lagged behind the Digital Network Industry. Data globalization also supports almost all of the international activities. The digital new era initiates a new "Internet revolution" almost between all-over traditional businesses. Suddenly every industry wants to catch this new wave, like retail, catering and carrying trade, those traditionally industrial companies will link their original businesses with the internet to trigger more effects in the market, then though the big data mining and analysis to obtain the feedback and adjust their strategies on the business. Under those kinds of circumstances, data flows are flourishing worldwide, and the internet shrunk the physical gaps in traditional goods trader that provide suitable surroundings for more countries and smaller enterprises launch E-commerce. This shift has far-reaching implications on the development of a digital economy.

In the perspective of the EU, the Digital Single Market will improve the international trade capabilities of SMEs in the EU and make the transborder trade and services more convenient. Before the DSM, only 7% of SMEs in the EU sell the goods or provide services cross-border, according to the account, 57% of corporations are willing or increasing online sales to the other Member States or other countries after several e-commerce policies applying. Not only that, but EU consumers could also save €11.7 billion each year if they could choose from a full range of EU goods and services when shopping online. Since that, the biggest problem which hindered the cross-border e-commerce seems is the 28 different national consumer protection and contract law,

[3] Economics, Oxford. "*Digital Spillover: Measuring the True Impact of the Digital Economy*." A Report by Huawei and Oxford Economics, Oxford, United Kingdom, (2017), available at: https://www. oxfordeconomics.com/recentreleases/digital-spillover .
[4] James Manyika et al., *Digital Globalization: The New Era of Global Flows*, vol. 4 (McKinsey Global Institute San Francisco, 2016).

numerous different restrictions on the cross-border make those companies exhausted to fulfil all the obligations in every Member States. More than that, the high costs of cross-border parcel delivery, unjustified geo-blocking in different Member State, the obstacles of copyright restrictions and value-added tax burdens also was headache problems to the cross-border e-commerce. According to the report of Commission,[5] the EU digital market consists of the national online services (42%) and US-based online services (54%), but the EU Cross-border online services represent only 4%. The EU has lagged behind the U.S. and China in the digital economy, let alone the global digital market. This strategy aims to reduce barriers to cross-border online commerce and strengthen the EU's competitiveness in the digital world economy.

Since that, the ambition of the Commission initiated the DSM strategy is unambiguous, according to the research of the Commission, the DSM strategy can create up to 415 billion Euro in additional growth, hundreds of thousands of new jobs, and vibrant knowledge-based society.[6] DSM strategy build-up the three pillars to achieve those objectives, the first pillar is "Access: better access for consumers and businesses to digital goods and services across Europe"; the second pillar is "Environment: creating the right conditions and a level playing field for digital networks and innovative services to flourish"; the third pillar is "Economy & Society: maximizing the growth potential of the digital economy".[7]

The DSM should address several issues like -'Boosting e-commerce', -'Modernizing the EU copyright rules', -'Revising audiovisual rules', -'Setting up the system and authorities to deal with the cybersecurity problems', -'Unblock the potential EU data economy', -'Improve the internet environment' and -'Adapting the ePrivacy rules and protect the data flow'. The following section will simply introduce the main contents of DSM.

1.1.2. The Main Contents of Digital Single Market[8]

Digital Single Market is amid to harmonize the different market between the Member State in the area related

---

[5] European Commission, "Why we need a Digital Single Market," *Factsheets on Digital Single Market*, 6 May 2015, available at: https://ec.europa.eu/commission/sites/beta-political/files/dsm-factsheet_en.pdf .
[6] European Commission, "Why we need a Digital Single Market," *Factsheets on Digital Single Market*, 6 May 2015, available at: https://ec.europa.eu/commission/sites/beta-political/files/dsm-factsheet_en.pdf .
[7] European Commission, "Shaping the Digital Single Market," available at: https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market .
[8] The contents of this section is based on the document of the Commission, European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A Digital Single Marker Strategy for Europe*, COM(2015) 192 final, 6 May 2015, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015DC0192 .

to the digital internet commerce, and it is a broad range blueprint, the following is main contents of DSM:

a) Remove the barriers in the regulations and administration to obtain a friendly and free environment for E-commerce. Firstly, the EU needs to harmonize and simplify the regulations of E-commerce. Since the situation that the EU lack of the consolidated regulations on the E-commerce at Union level, the Commission will publish several new regulations of online purchase to regulate and unite the rules in the Member States, then pushing them to revise the related regulations in domestic level in order to shrink the gap of regulations between the different regions, and the Commission will be based on the current situation of Internet development to reform the "Regulation on Consumer Protection Cooperation" which published at 2007. All those measures are in order to establish a convenient and normative climate for E-commerce and promote the transparency of the online purchase information. Secondly, reduce tax burdens to Internet companies. The Commission is working on the revise and simplify the regulations about VAT (Value Added Tax) and set up a series of tax reduced systems for the SMEs and new setup companies which work on the digital commerce area. Meanwhile, the Commission will promote the mechanism that digital products producer could declare and pay the VAT at the original place in onetime, no need to finish those works in different sales place.

b) Strengthen the management of the online platform. Based on the research of the Commission, the network platform has become the core position of the digital economy step by step. Therefore, the Commission has an obligation to enact policies to lead this industry going on a steady and healthy developing way. Besides, the Commission will evaluate the status of development of the online platform based on the elements like the transparency of operation, the relationship between the platform services provider and suppliers, and process of consumers' information, after that, the Commission will proceed in accordance with the results of the evaluation to advance the amend opinions. In the meantime, the Commission will put the online platform into the jurisdictional limit of the competition law and set up the "European Union online platform round table" to promote the cooperation on the online platform and focus on the issue of data security and protection. In order to deal with the international cyber-attack and the other challenges which be brought by the features of the Internet itself and advanced the standards of the supervision of the data security, the Commission would push the "*Network and Information Security Directive*"[9] to

[9] (This proposal already been passed and published) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, *concerning measures for a high common level of security of network and information systems across the*

come out and into force, establish a framework about Public-Private Partnership on Cybersecurity in the area which aimed for the technologies and solutions for online network security. For the protection of personal information this vital content of DSM, the Commission will review the ePrivacy Directive[10] to adopt the regulations and current situation of the network in one level, since the last update was 2009.

c) Improve the Telecommunicational and Audiovisual market's environment. For the telecommunicational industry, the Commission will formulate the new version of the regulatory framework for electronic communications to combine the online services, services support, and consumer protection together; promote the measures to cancel the high roaming charging of telecom and data transfer when they cross the border between the Member States in the EU territory. For the Audiovisual industry, the appearance of a new digital era brings incredible changes to the traditional Audiovisual business, the numerous internet contents and services provider suddenly came into the ground, and those new digital companies also bring the new business models to this industry, the "ancient rules" already failed to catch up that new wave and regulate those new situations, under this circumstances the Commission will overhaul the "*Audiovisual Media Services Directive*"[11] to fit the new business model for the content distribution.

d) They are pushing the reforms of digital and internet technologies. Firstly, promote the development of Big Data and Cloud Computing, the Commission will propose to initiate a plan named "Free flow of data" in order to tackle the issues about eliminate the technical and juristic obstacles on the data flow, resolve the problems about proprietary of data and the liabilities ascription of data flow, and enhance the support for the research on Big Data. Secondly, the Commission will focus on the interoperability and standardisation of digital information. The interoperability is amid to ensure effective and feasible communications between different digital components and provide free access for the different industry in different regions. In order to achieve those objectives, the Commission will update and extend the "European Interoperability Framework" and courage the Member States to set up the database, allow users to freely choose and change Internet service provider without technical restrictions and sharing the

Union, OJ L 194, 19 July 2016, pp. 1–30.

[10] Directive (EC) 2002/58/EC of the European Parliament and of the Council of 12 July 2002, *concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, OJ L 201, 31 July 2002, pp. 37–47.

[11] Directive (EU) 2010/13/EU of the European Parliament and of the Council of 10 March 2010, *on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)*, OJ L 95, 15 April 2010, pp. 1–24.

cross-border data through a smooth way. Thirdly, accelerate the development of E-government services. The Commission will formulate a new E-government Action Plan 2016-2020 which will include: (1) Initiate the "Europe Single Digital Gateway Plan" and unified entry point at the EU level; (2) Launch the "Once-Only" principles which a principal could offer quality and effective public administrative service, "Once-Only" principal means the citizens and companies will only apply their information once to any Member States' administrative body and no need to provide again when other administrative body needs that information, they should search those related data on the internal network; (3) Accelerating Member States' transition towards full e-procurement, interoperable e-signatures and sharing the companies registration information.

e) Increase the investment of digital network industry, and the EU public investment will play a lead role when they are extending the influence of the digital network industry. The European Structural and Investment Funds already funded EUR 21.4 billion on areas like infrastructure, research programs, and innovative SMEs. Meanwhile, the European Investment Bank and the European Investment Fund will also support significant additional funding to those works, and the Commission will provide the legal basis for the highly innovative companies to get financing opportunities through establishing the "European Venture Capital Funds Regulation".

1.2. Data Security is the Basic Structure for the Digital Single Market

1.2.1. Trust and Security are at Core of the Digital Single Market Strategy

At 27 April 2007, a series of cyberattacks aimed to several websites of Estonian organisations, the parliament of Estonian, banks, mass media, and other organisations' network has been attacked and crashed, then those websites have resorted after three weeks, it caused uncountable loss to Estonian. The *2007 cyberattacks on Estonia* has become the milestone of Europe Network Security Policy because it ringed the alarm for other States.[12] In 2013, Edward Snowden disclosed a huge scandal of the United States National Security Agency (NSA) in this century, the PRISM surveillance program. The NSA through PRISM to monitor the digital

[12] Ottis, Rain. "Analysis of the 2007 cyber attacks against estonia from the information warfare perspective." *Proceedings of the 7th European Conference on Information Warfare*. 2008.

network information of Europe, even the prime minister of Germany Angela Merkel's phone also been tracked and monitor. And the PRISM scandal introduced numerous impacts to the world, including the collapsed of the Safe Harbor Framework which a provision of personal privacy information transborder flows between the European Union and the United States (The details of Safe Harbor Framework is in the Next Chapter).[13] During 2017, several malignant cyberattacks destroyed the public's confidence in Data Security, in May, the WannaCry worm hijacked numerous windows user, and it spread nearly hundreds of countries.[14] At July, a new Petya worm outbreak and at October, a virus named "Bad Rabbit" continue raging the internet world, all those ransomware epidemic locked the computer which has been infected, and those hackers threatened the owners they will destroy all the information and documents if they could not get the ransom bitcoin.[15] All those malignant cyberattacks bring tremendous loss to the finance and striking the political stability of the European Union, and it also added potential destabilising factors to the society.

Nowadays, private and business life almost relies on the modern Information and Communication Technologies (ICTs), everything links with the internet, social media, online shopping and delivery, network support to the traditional industries, etc. According to the statistics from the EU Cybersecurity Dashboard[16] and Eurobarometer[17], the ICTs industry directly contributes 5% GDP to Europe, that is nearly 600 billion Euros market value, and stimulate and protect the development of the DSM. However, the EU faced more than 5000 times threaten from the ransomware epidemic in every day and the cybercrime already beyond half of the criminal cases. Undoubtedly, the Cybersecurity has become the most sensitive and important issue which hinder the step of the Digital Single Market. On 3 March 2010, the Commission published the "*EUROPE 2020 A strategy for smart, sustainable and inclusive growth*". The DSM strategy is aimed at achieving the Europe 2020 Strategy, which has seven pillars; the DSM strategy is one of them. Besides, the other pillar is the strengthening of online trust and security, and it is also the core measure of the DSM strategy.

---

[13] Penney, Jonathon W. "Chilling effects: Online surveillance and Wikipedia use." *Berkeley Tech. LJ* 31 (2016): 117.
[14] Dwyer, A. C. "The NHS cyber-attack: A look at the complex environmental conditions of WannaCry." *RAD Magazine* 44 (2018).
[15] Orkhan, Mamedov; Fedor, Sinitsyn and Anton, Ivanov, "Bad Rabbit ransomware." *AO Kaspersky Lab*, (2017), available at: https://securelist.com/bad-rabbit-ransomware/82851/ .
[16] Dashboard, EU Cybersecurity. "A Path to a Secure European Cyberspace." (2014).
[17] Eurobarometer, Special. "390-Cyber Security Report." Publication: July (2012); & EU Commission. "Special Eurobarometer 423: Cyber Security Report." (2015).

1.2.2. The Principles of the Cybersecurity Strategy of the European Union

The borderless nature of the Internet and the multi-layered nature of users have made the Internet deeply penetrate social life. The private sector plays an important role in the use and maintenance of the Internet. However, maintaining the security, stability, and transparency of the Internet still requires the public sector to play a functional role, establish policies and regulations, and combat the illegal threats to cybersecurity. The EU has followed five guiding principles in the development of the Cybersecurity Strategy.

a) The core values, laws and regulations of the EU also apply to the virtual cyberspace. The purpose of cybersecurity is ensuring the peace lasting in the cyberspace, then achieve sustainable development to the society and economy of the EU, to help citizens achieve their personal values, and to establish common values such as equality, fairness, and the rule of law in the cybersecurity framework.

b) Protection of the fundamental rights of people, rights to free speech, data of personal information and privacy. The cybersecurity strategy is only durable and effective based on the fundamental rights and core values which regulated in the EU treaties. The individuals' fundamental rights cannot be guaranteed if without the safety and effective network information system. When the situation for cybersecurity puts the shared personal information in an unsafe condition, it should also comply with the EU data protect regulations and fully respect the individual's rights and interests.

c) Ensure the functional network access for all of the users. Due to the high popularity of the network in society, any restrictions or prohibition of users accessing the Internet will cause a negative impact on citizens' digital life. The EU must ensure the integrity and safety of the internet while maintaining cybersecurity, and cannot hinder the free movement of data flow, besides ensuring every user could securely access the internet.

d) Establisher a democratic and efficient system to encourage more multi-stakeholders to participate in cybersecurity. The cybersecurity always not controlled by the single entity. Usually, it's linked with the participation of numerous multi-stakeholders. From a perspective of the cybersecurity management, the non-government organizations and industry itself involved in the management of internet resources,

network protocols, and standards has become the norm, that shape the future of the Internet.

e) It is clarifying the responsibility assignment of the cybersecurity. Nowadays, in almost all areas of social life depends on the ICTs, that really provide the convenience and effectiveness to the peoples, however, in another sentence, the ICTs also put the pubic into a vulnerable circumstance. Therefore, it is necessary to correctly understand and analysis of current cybersecurity's situation, then remedy the potential risk timely and reduce damage to cybersecurity. Whether it is the individual, organizations or the public departments, all network participants should assume the joint responsibility of cybersecurity and take a coordinated response to strengthen the security of the Network industry.

The Digital Single Market is aimed to provide better digital products and services to Europe citizens and corporations to achieve the free movement of goods and services which transborder flows and create a convenient, fair, and transparent competitive environment for the digital network and creative services, and to maximize the potential growth of the digital economy. However, the cybersecurity problems have increased the concerns of users while they living on the Internet, and the current maturity level of cybersecurity cannot catch up with the requirements of Digital Single Market and Smart Europe.

When the European Union transform to Smart Europe, the cybersecurity is not only the technical pillar for the DSM but also the safeguard for the Single Market for the European Union. Only when the cybersecurity has been maintained in safe surroundings, the personal data could be protected, the risk of corporate information system being attached will be reduced, and critical infrastructure information systems will be protected. Then, the Europe society could feel the benefits brought by the innovation and digitalisation in the digital industry, and increased acceptance of digital industry will stimulate the new consumer demands in this area.

The cybersecurity and data protection undoubtedly is one of the basic structures of the Digital Single Market, among those issues which need to deal with in data protection area, the security of the data flow in the digital world is the most urgent issue that needs to be dealt with,[18] especially when those data linked with the personal information and when it transborder flows, the transborder data flows linked numerous data subjects and

[18] Lucas D Introna, "Privacy and the Computer: Why We Need Privacy in the Information Society," *Metaphilosophy* 28, no. 3 (1997).

sensitive information and the routes of data flow are tremendously complex and uncontrollable,[19] the transborder data flow has become the eyebrow-burning issue of the data security area.

1.2.3. The Role of Transborder Data Flows in Data Protection System

Nowadays, almost everything could link with the internet, and numerous data flows in it, among that tremendous information the 'sensitive data' seems the most valuable information to the many subjects, like state intelligence agency, multinational corporation and the Internet Service Provider (ISP). Those "sensitive data" always include personal information or secret information to the company or the state.[20] Lucas d. Introna believes that personal information will lose control when it flows into the digital world, more and more individuals will communicate via the electronic media to get access to the information subject, then information subject will progressively lose control over the ability to clearly structure of social roles.[21] That means if data subject cannot handle the relations of roles in the digital world and the real world, it will cause the data subject to lose themselves and fall into the "black hole" of the social role. That is only just the personal data if those data link with the business secret numerous companies will be restricted by other competitors if those data link with the state's security and leakage to the other regimes' intelligence agency or terrorist organizations that outcome will be unimaginable.[22] In order to construe a suitable atmosphere for the digital network, the data transfer and data process as the basic means are really important to deal with those issues. In many areas, the transborder data flows removed the barriers of geo-blocking in the digital and internet level,[23] makes the four freedom of movement 'freer' and these kinds of superiority also fulfilled with the objectives of the DSM.

Nonetheless, the Transborder Data Flows also faced several high risks, such as 1) The leakage of personal privacy data and the important data. (which linked with the state security and public interest) 2) The monitor

---

[19] Zhang YuAn and Song Kai, "Thoughts on the Risk of Cross-border Flow of Data in the New Period," *ZhongGuoXinXiAnQuan*, no. 11 (2018).
[20] McKay Cunningham, "Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law," *Geo. Wash. Int'l L. Rev.* 44 (2012).
[21] Introna, Lucas D. "Privacy and the Computer: Why We Need Privacy in the Information Society." Metaphilosophy 28, no. 3 (1997): 259-75.
[22] Cunningham, McKay. "Privacy in the age of the hacker: balancing global privacy and data security Law." *Geo. Wash. Int'l L. Rev.* 44 (2012): 643.
[23] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A Digital Single Marker Strategy for Europe*, COM(2015) 192 final, 6 May 2015, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015DC0192 .

of the intelligence agency of a foreign regime or an international organization. 3) The difficulties of domestic enforcement. 4) Uncontrollable development of local protectionism.[24] The widespread and application of ICTs at a certain point boosting the personal information transborder flows become normal, those data which cross the borders of the traditional physical state are using the "control right" which weakened and attached to the data. This "control" both include the control right of the data subject which base on the data ownership and the control right of states which base on the data sovereignty. Once the data out of control, especially when the data recipient states lack the essential ability on data protection, the data will face risks like collect, access, process, disclosure, and distort under the unauthorized conditions.[25] Therefore, the states will go through the legislation to regulate the Transborder Data Flows and achieve the different demands from the different parties.

a) The demand for personal information protection. The new technology in ICTs areas like big data, cloud computing, and block-chain are promoted the flow and convergence of personal data, the economic value of the data flow is keeping climb to a new peak. The personal information data not only become a vital element for the corporations to achieve profit maximization but also as the core part of the critical infrastructure of states. The value and importance of personal data determine the high probability of being infringed, on the one hand, personal data is "favourite meats" to the terrorists and crimes, the global data black industry is becoming more and more actively, and the phenomenon of malicious use and trading of cross-border data is frequent, and personal data leakage continues to occur. On the other hand, companies tend to charge and process a mass of personal data to take a position in the market, which puts higher demands on the security of personal data. Moreover, the requirements and conflicts of compliance have further exacerbated the security risks of personal data, and the integrity and confidentiality of personal data have been hit by unprecedented impact. Perfecting the unified rules to ensure the safe flow of personal data has also become an inevitable demand for regulatory legislation.[26]

b) The demand for convenient enforcement. The Transborder data flow makes large amounts of data flow abroad, it takes more time, and human resources for law enforcement agencies to extract valuable

[24] Kuner, Christopher. "Reality and illusion in EU data transfer regulation post Schrems." *German Law Journal* 18.4 (2017): 881-918.
[25] Daoli Huang, and Zhile He, "'Big Data Phenomenon' of US and EU Data Cross-border Regulation Legislation and Enlightenment for China," *Journal of Intelligence* 4, 2017.
[26] Daoli Huang, and Zhile He, "'Big Data Phenomenon' of US and EU Data Cross-border Regulation Legislation and Enlightenment for China," *Journal of Intelligence* 4, 2017.

evidence, and the challenge of efficiently identifying data is even greater, which means the data abroad will increase the cost of enforcement. To make up for the lack of jurisdiction over transnational crimes and improve the convenience of law enforcement, it is necessary and appropriate to supervise the cross-border data, such as the requirement to implement mandatory backup before transborder data flow, which becomes an inevitable demand for regulatory legislation.[27]

c) The demand to maintains the sovereignty of the states. The ability of the country to own the scale flows and utilization of data will become an important component of comprehensive national power. Data is an important strategic resource to support national security and development and has an extremely significance value of sovereign protection. The Transborder Data Flows is inevitable, however, for allover countries in this sphere, especially the countries that leg behind the modern informatization technologies and incomplete legislation, it will directly pose serious challenges to the integrity of national sovereignty.[28] How to adjust the supervision mechanism of Transborder Data Flows, and solve the conflict of rights in the process when cross-border data flows and the objection of data jurisdiction. All those issues make the regulatory legislation become the necessary demand for national sovereignty maintenance.

From a macro-level perspective, all those strategies like the DSMs and Data Protection Strategy are served for the politics, economy, and stability of society. The personal information data flows cross-border has a strong connection with the individual's interest. Therefore, the protection of this area becomes more and more important. And the regulations on the Transborder Data Flows not just come out in near, its already regulated several decades and keep adapting to align with the changes of the ICTs field.

[27] Yue Shi, "The Management of Transborder Data Flow Under the Digital Economy," *Information Security and Communications Privacy* 10, (2015).
[28] Mengshan Ren, "The Information Space and Geographic Space: the Internet Communication and National Sovereignty," *Modern Communication* (*Journal of Communication University of China*), 6, 2011.

2. Chapter Two: The Legislation of Transborder Data Flows on Personal Information in Europe

2.1. The Separate Legislative Period on Protection of Personal Information in Europe

The 70s and 80s of the last centuries, many Europe countries started to legislate on personal data protection. During this period, the legislation on personal data protection is still in the start stage, and those countries are focus on the different fields, like privacy, individual information and personal data. Such as Belgium, focus on personal privacy; the Austria and UK focus on the individual information; the France, Germany, Iceland and Norway mainly focus on the personal data.[29] The concept and value orientation of personal data are ambiguous is an important reason for the difference in the legislation direction of personal data protection.

(1) The Legislation of Personal Data Protection Law in Germany

At 1970, West Germany published the first comprehensive personal data protection law on the worldwide, the "*Hessisches Datenschutzgesetz*",[30] it regulated the use of personal data by public administration agencies. However, it is not regulated the issues of Transborder Data Flows on personal data. The Frankfurt is the largest city in Hessen and the financial centre of Europe at that time, the relatively frequent use of personal data for commerce was quite popular, in order to adjust the use of personal data by relevant industries and public administration, the "*Hessisches Datenschutzgesetz*" has been published at 1970. Subsequently, at 1977, the Federal Republic of Germany had enacted the "*Bundesdatenschutzgesetz*" (BDSG), the Federal Data Protection Act, at the national level to adjust personal data protection and its related field.[31] However, the legislation in this period is still unclear in terms of purpose, content, and rights. For example, from the perspective of legislative purpose, "protecting the 'worth protecting interests' while abusing personal data in the data processing" are fails to clearly indicate the object to be protected, and the legislative purpose is

[29] Aiming Qi, The Legal Issues Research on Personal Information Protection Law and Transborder Data Flow, Wuhan University Press, 2004.
[30] Germany, Hessisches Datenschutzgesetz, (Hessen Data Law), 7 October 1970.
[31] Riccardi, J. Lee. "The German Federal Data Protection Act of 1977: Protecting the right to privacy." *BC Int'l & Comp. L.* Rev. 6 (1983): 243.

ambiguous; from the perspective of the scope of application, the BDSG only regulated the resolutions of abuse problems after the personal data has been collected but not referred to the protection before the collection; from the perspective of an application object, the BDSG only restrict the public administration when they are processing the personal data but not regulated the other objects, like individuals and companies.[32]

(2) The Legislation of Personal Data Protection Law in the United Kingdom

In 1974, the United Kingdom formulated the "*Consumer Credit Act*", which focus on the personal credit information, it covered several relevant contents of personal data protection, but this act only deals with personal data that is publicly processed in the field of consumer credit, and the object of protection is only personal data related to personal credit transactions and is processed manually.[33] In 1984, the UK published the "*Data Protection Act*" which extended the subject of personal data protection to all existing data that connect with individual and automatically processed. And set up the Data Protection Registrar system; limited the scope of collecting and processing data under explicit and legal purposes; prohibited to transact the personal data out of the UK directly or indirectly; extended the data subject's rights, like the right of data publication, right of rectification and the right to claim compensation for the loss.[34]

(3) The Legislation of Personal Data Protection Law in France

France enacted the "*Act N°78-17 of 6 January 1978*, *on Information Technology*, *Data Files and Civil Liberties*" in 1978. Compared with Germany, Sweden and other countries on the legislation of personal data protection, the French "1978 Act" is more specific and detailed, it regulated the procedures to application and authorization of data process, and the rules should be followed, meanwhile, set up the National Commission on Informatics and Liberty as a supervisory agency and clarified the legal content that personal data belongs to natural person owner and they has the right to access their personal data.[35]

It is not hard to find in that period, although those traditional regulations in Europe have several differences in notions, the scope of application or supervision, all of them are formulated based on a common value, that

---

[32] Hornung, Gerrit, and Christoph Schnabel. "Data protection in Germany I: The population census decision and the right to informational self-determination." *Computer Law & Security Review* 25.1 (2009): 84-88.
[33] Wilson, Therese, Nicola Howell, and Genevieve Sheehan. "Protecting the most vulnerable in consumer credit transactions." *Journal of Consumer Policy* 32.2 (2009): 117-140.
[34] Bennett, Colin J. *Regulating privacy: Data protection and public policy in Europe and the United States*. Cornell University Press, 1992.
[35] Hondius, Frits W. "Data law in Europe." *Stan. J. Int'l L.* 16 (1980): 87.

is protect the privacy. That is the protection of human rights. Besides, it formed the cornerstone of legislation of personal data protection on the EU and leading the development of personal data protection in the future.

2.2. The Historical Development of Legislation of Personal Data Protection on the European Union

Actually, the regulations of personal data protection on Europe at the 70s of last century were only adapted to the electronic data technology that was just beginning, the World Wide Web and ICTs are the faraway future at that time. Limited by the technological barriers, the data storage and distribution were relatively tradition and simple at that time, the large-scale storage devices or paper documents are the main patterns, that caused the ineffectiveness on data transaction.[36] In this context, the early regulations of personal data protection on Europe were mostly to protect individuals' fundamental rights to personal data and rarely referred to the Transborder Data Flows on Personal Data.

However, with the development of science and technology, the emergence of data miniaturization storage and the Internet makes it possible for personal data to transborder flows easily and in large numbers. Once the data is out of the country, the domestic personal data protection mechanism will be beyond the reach. Meanwhile, numerous countries still have not established the personal data protection system in domestic or already established, but protection mechanism is faultiness and combined with the huge gap between countries on the economy, politics, and culture. All those difference between the countries or areas may trigger conflict on personal data protection, then the personal data which crossed the border will face infringements or other risks. The protection and remedies of personal data seem like a "mission impossible" if only rely on domestic regulations. After recognized the limitations of domestic law, many international organisations started to formulate personal data protection conventions at the domestic or international dimension to maintain the free flow of personal data and to protect the rights of the data subject. The conspicuous difference compared with the domestic regulations is that international conventions not only protects the rights of personal data but also focus on the promote the free flow of personal data as legislative intent. [37]

---

[36] Kirby, Michael D. "Transborder Data Flows and the Basic Rules of Data Privacy." *Stan. J. Int'l L.* 16 (1980): 27.
[37] Rudraswamy, Vanishree, and David A. Vance. "Transborder data flows: adoption and diffusion of protective legislation in the global electronic commerce environment." *Logistics Information Management* 14.1/2 (2001): 127-137.

As an initiator of free flow on data cross-border, the OECD passed and published the "*Guidelines Governing the Protection of Privacy and the Transborder Flows of Personal Data*"[38] at 1980. However, the OECD Guidelines does not focus on data protection, nor does it intend to protect personal privacy. Instead, it aims to ensure the safety and sustainability of cross-border flows of personal data among participants of OECD, and it treated the domestic legislation on data protection as the protectionist legislation and non-tariff trade barriers. Despite the fact that the OECD Guidelines is promoted the transborder data flows, the shortcomings of the OECD Guidelines are also obvious, in the one hand, although the Guidelines are flexible, the guidelines are not binding legal documents, and member states have no statutory obligations to implement, in the other hand, the broad exemptions contained in the Guidelines restrict its effectiveness. Therefore, the legal effect of the Guidelines is limited, and the legislative difference still exists in the Member States.[39]

2.2.1. The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108)

In the development of data protection in Europe, the Council of European Union played a lasting and far-reaching impact. The Council of European Union is aimed to protect the priority of human rights parliamentary democracy and rights in Europe and reach an agreement in Europe to coordinate social behaviours and legal act of all Europe countries and promote the unity of European culture. The "*European Convention on Human Rights*" which formulated under the framework of the Council of European Union and published at 1950 include the provision of privacy, and the ECtHR (European Court of Human Rights) through expanding interpretation made that provision also functions to protect personal data.[40] Then, in the 1970s, the Council of European Union focused on expressing political opinions and regarded personal data as part of Article 8 Para 1 of the ECHR. At the meantime, asked the Committee of Ministers to review the domestic law and the

---

[38] OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)", available at: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm .

[39] OECD, "Policy Issues in Data Protection and Privacy," *OECD Informatics Studies*, No. 10, OECD, 1974.
The purposes of OECD Guidelines include: 1. Achieve the recognition of minimum standards on protection of personal privacy data; 2. Reduction of differences in legislation and practice among member states; 3. Avoiding improper intervention among personal data flow; 4. Minimize the barriers to cross-border data movements in Member States.

[40] De Hert, Paul, and Serge Gutwirth. "Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action." *Reinventing data protection?*. Springer, Dordrecht, 2009, pp. 3-44.

ECHR in the Member States and determine if and to what extent protect individuals from risk.[41] At 1981, the Council of European Union formally published the "*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (*Convention 108*)"[42] and in force on October 1,1985. *Convention 108* is a groundbreaking regulation in European data protection system. However, the *Convention 108* is a non-self-executing treaty which means it demands the Member States' domestic legislation to implement, before the domestic legislation the Convention 108 is not binding on the Member States. In 1981, the Council of European Union recommended that the Member States ratify the *Convention 108* by the end of 1982 and retaining the right of recommendation if they were not ratified. However, until 1989, only seven Member States had ratified the *Convention 108*.[43]

Convention 108 as the first binding international convention on the protection of personal data set up the basic rules on transborder flows on personal data. The most meaningful point of rules which regulated the transborder flows on personal data is that coordinates conflicts between personal data protection and the free movement of cross-border data flow. Technically, *Convention 108* only regulated the fundamental principles and standards on Transborder Data Flows and left the implementation issues to the Member States. That not only unified the bottom line of rights but also ensure consistency of fundamental principles and standards between the domestic regulations and laws and provides the discretion for the domestic legislation of each Member States, so that avoid the conflict between the *Convention 108* and the domestic laws in the Member States. It is for these reasons the *Convention 108* had a profound impact on legislation in other regions and later the Data Protection Directive.

---

[41] Council of European Union, *Convention for the Protection of Human Rights and Fundamental Freedoms*, ETS 5, 4 November 1950; Council of European Union, Parliamentary Assembly Recommendation 509, *Human Rights and Modern Scientific and Technological Developments*, 31 January 1968.

[42] European Commission, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data," opened for signature January 28, 1981, European Treaty Series no. 108, https://rm.coe.int/CoERMPublicCommonSearchServices/ DisplayDCTMContent?documentId=0900001680078b37 .

[43] European Commission, Commission Recommendation of 29 July 1981 Relating to the Council of European Union, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, OJ L 246, 29 August 1981, p.31.

2.2.2. Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data

With the concerns that difference between the data protection laws of Member States will hinder the development of the internal market, the Council of European Union published a series of proposals for directives which include the "*Proposal for a Council Directive concerning the Protection of Individuals in Relation to the Processing of Personal Data*"[44] , and the Commission pointed out that the lack of the laws in the Member States is unable to reflect the commitment of the protection of the fundamental rights of the Community.[45] The Proposal of DPD drawn a lesson from the *Convention 108* that ordinary directive cannot achieve the desired results and followed the values of the OECD Guideline on limiting data processing and data protection. After five years of negotiations, in 1995, the milestone of data protection in Europe has come on the ground, the "*Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data* (the Directive)".[46]

The Directive unambiguously shows the legislative concept of the protection of personal data to the world. Compared with the previous regulations on the protection of personal data in Europe, the Directive has strict rules on the personal data processing criteria; setup the clear and definite rules on the protection of personal data; expanded in terms of the specific scope of application; focus on the implement in the regulatory enforcement.[47] It is not difficult to find that the Directive attempts to protect personal data from all aspects of transborder flows of personal data, from these specific legal texts. In particular, the Directive developed an original mechanism which differences between the internal and external domain to solve the inevitable contradiction between the protection of personal data and the free movement of data. For the internal conditions which the personal data flows between the Member States, the Directive required the Member States not only protect the fundamental rights on transborder flows of personal data but also prohibited the restriction on the free movement of data flow on the pretext of data protection. For the external conditions

---

[44] Council of the European Union, *Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data*, COM (1990) 314-2, *OJ* C 277, 5 November 1990, pp. 3-12

[45] European Commission, the Communications from the Commission to the Council, *Community policy on data processing. Communication of the Commission to the Council. SEC (73) 4300 final*, 21 November 1973.

[46] 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, *OJ* L 281, 23 November 1995, pp. 0031-0050, http://data.europa.eu/eli/dir/1995/46/oj .

[47] Lynskey, Orla. *The foundations of EU data protection law*. Oxford University Press, 2015.

which the personal data will cross the EU's border and flows to the third countries, firstly, the Directive is forbidden that the Member States transfer the personal data to the third countries that lack an adequate level of personal data protection; secondly, clarifies the exceptions on the first condition; thirdly, regulated the "Standard Clauses Contract" and other workarounds to set the flexible clauses.[48]

The Directive as the main legal instrument of personal data protection on Transborder Flows has the dominant position in this field. The "adequate level of protection" that the Commission will assess whether third-party or region meets EU requirements have had a profound impact on the establishment and improvement of personal data protection systems in numerous countries and regions. Not only that, but at the specific context on the implementation, the Standard Clauses Contract and Binding Corporate Rule also provide more feasible options for some large transnational enterprises on the protection of transborder personal data flows. [49]

2.2.3. The General Data Protection Regulation

The Directive actually only provided a supervisory framework on data protection; all Member States still need to base on the Directive to legislate domestic law. It caused the divided situation of Member States' domestic law which under the unified Europe internet supervisory framework. Since the different conditions between the Member States, the purposes, background and consideration also will different and caused the gap between the personal information protection regulations of Member States. Besides, the Information and Communication Technology are highly developing and spreading, the brand-new technologies like the Big Data, Blockchain and Cloud Computing also came out in a near decade, the Directive is hard to catch the wave of time and leave a number of blanks that need to be regulated the new situations which brought out by the new technical revolution.

At 2010, the Vice-President of the Commission Viviane Reding made a speech at the European Data Protection and Privacy Conference, she mentioned that although the EU has the best data protection law in the world, however, the highly developing on technology also will bring the new challenges and problems. Nowadays,

---

[48] Simitis, Spiros. "From the market to the polis: The EU directive on the protection of personal data." *Iowa L. Rev.* 80 (1994): 445.

[49] Kuner, Christopher. "Regulation of transborder data flows under data protection and privacy law: past, present, and future." *TILT Law & Technology Working Paper* 016 (2010).

privacy issues already become a mobile target that the new risk needs to be repaired by law enforcement.[50] And with the financial crisis in 2008, the Europe economy also got the hit and peoples are suffering, in order to rebuild the economy and inspire the citizens, the EU published the 2020 strategy, and five main goals, one of them is the Europe Digital Agenda which aim to push the developing and widespread on high-speed internet and build the DSM.[51] Under this kind of circumstances, the Commission established the proposal of GDPR in 2012,[52] through the four years negotiation, at 2016, the Parliament and Council passed the GDPR, and it has enforced at the May of 2018.[53]

2.3. The Early Structure of Transborder Data Flows on Personal Information

The Directive builds the basic structure of Transborder Data Flows on Personal Data in Europe and established two fundamental goals: First, reached a unified minimum level of personal data protection in the EU; Second, remove the barriers and restrictions to ensure the personal data free flows internal of the EU.[54] The Article 25 of the Directive is a general principle of Transborder Data Flows on Personal information, and it requires that only when the adequate level of protection of personal information fulfils the EU requirements, then the Member States could transfer personal information to a third county. Article 26 is the exceptions of adequacy decision which has two parts. The first part is the statutory exception which is to take into account the existence of other legal interests that take precedence over personal information and therefore set exceptions of the adequacy decision. The safeguard measures are the second part which aims to protect the personal data transborder flows between specific individuals, corporations, and organisations when the receptor country was failed to meet the requirements of the EU's adequate level of protection. There are three types of safeguards that have been regulated under the Directive, the Standard Clauses Contract (SCC), the Binding Corporate

---

[50] Reding, Viviane. "Why the EU needs new personal data protection rules?." *The European Data* (2010).
[51] European Commission, “Europe 2020 strategy”, https://ec.europa.eu/digital-single-market/en/europe-2020-strategy .
[52] Proposal for a regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
[53] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (*General Data Protection Regulation*) (*Text with EEA relevance*), *OJ* L 119, 4 May 2016, pp. 1–88.
[54] 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, *OJ* L 281, 23 November 1995, pp. 0031-0050, http://data.europa.eu/eli/dir/1995/46/oj .

Rule (BCR), and the Safe Harbor Framework.

2.3.1. The Adequate Level of Protection

The adequate level of protection is the general principle of transborder data flows on personal information which based on the Article 25 of the Directive that required only when personal data protection of the third country fulfil the requirements of the adequate level of protection then the Member States could transfer the personal data cross-border to the third county. The thing should be mentioned is that the adequate level of protection not means if the third county reached the adequate level of protection the personal information cross-border transfer will not exist any limitations, actually it only means the Member States could not prohibit the transfer on the ground that the third countries are failed to obtain the adequate level of protection of personal information. Put it in another word, that means the transfer personal information across the EU border not only should meet with the requirements of the adequate level of protection but also need to fulfil the requirements of transborder data flows on personal information which lay down on the domestic law of Member States.[55] For example, Article 6 of the Spanish Data Protection Act regulated that the transfer and process of personal data should obtain the consent of data subject. The data controller demands to fulfil two requirements if they transfer the personal data from Spain to the third country which out of the European Union, the third country need to obtain the adequate level of protection of personal information, and the Controller should be got the consents of every data subjects. Undoubtedly, those requirements are heavily burdening for the corporations that need to transfer the personal data cross-border.

According to the Article 25 para.6 of the Directive, the Council and the Parliament transfer the supervisory authority to the Commission which needs to estimate whether the third county could fulfil the requirements of the adequate level of protection. And the Commission will base on the Article 25 para. 2 to review a series element on the adequate level of protection[56]. However, the Directive only regulated the review element of the adequate level of protection but not confirm the standards and measures of assessment. The reason why the Directive does not clearly state the criteria and methods for determining the adequate level of protection of a third country is that it is difficult to list a uniform set of rules for evaluation, taking into account the

[55] Kuner, Christopher. *European data protection law: corporate compliance and regulation*. Vol. 20. Oxford: Oxford University Press, 2007.

[56] Directive 95/46/EC, *OJ* L 281, 23 November 1995, Article 25.

different legislative systems of each country. In federal countries such as the U.S. and Canada, the situation is more complex; the laws governing personal data protection vary from state to state.[57] Therefore, the Commission is more inclined to judge the adequate level of protection criteria by case identification. In order to give clearer guidance on the identification of individual cases, the Article 29 Working Party issued a guidance document in 1999 which lists the principles that the Article 29 Working Party considered in determining of the legal system for personal data protection in third countries.[58] Besides, the Article 29 Working Party also lists the elements which need to be evaluated on the enforcement of the third county's personal data protection laws.[59]

However, the Adequate Level of Protection still exist several defects and also faced numerous challenges on the enforcement. Firstly, the countries and regions that reached an adequate level of protection still less. Until present, only 12 countries or regions received the certification to get in the "white list" of the adequate level of protection which assessed by the Commission and based on the legislative status, enforcement capacity and judicial redress of third country or region. The Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay as providing adequate protection, the transfer of personal data to those countries or regions will be assimilated to intra-EU transmissions.[60] However, the six of those countries or regions belongs the Europe Continent, and other countries cannot represent the worldwide, only Japan and Canada has that ability, but the convention between the EU and Canada still limited in a specific area, The coverage area of the adequate level of protection is extremely limited, which weakens the adequate level of protection certification system as a macro-guidance of the general rules and cannot fulfil the requirements of the EU's cross-border transfer of personal information worldwide.[61] Secondly, the certification process is complex and tardy. The Commission's assessment of an adequate level of protection on third country or region needs a series complexity process. That demands the Commission intimate a proposal of assessment, then the Article 29 Working Party will provide analysis and

---

[57] European Commission, Data Protection Working Party, WP4: *First orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy*, XV D/5020/97-EN final, 26 June 1997, p.3.
[58] European Commission, Data Protection Working Party, WP12: *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, DG XV D/5025/98, 24 July 1998, p.5.
[59] European Commission, Data Protection Working Party, WP12: *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, DG XV D/5025/98, 24 July 1998, p.6.
[60] European Commission, *Adequacy decisions-How the EU determines if a non-EU country has an adequate level of data protection*, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en .
[61] Bennett, Colin J. "The adequacy of privacy: The European Union data protection directive and the North American response." *The Information Society* 13.3 (1997): 245-264.

identify the detail of the situation of the third county, after that, the Article 29 Working Party will submit the recommendations to the Committee of Article 31 for deliberation, at last, the Commission will be based on the results of deliberation to determine whether approve the certification or not. The certification process is really cumbersome and endless, taking New Zealand as an example, the Commission starts to evaluate the protection level of personal data on New Zealand from 2005, until 2011 the Article 29 Working Party just submit the recommendation, and the Commission affirmed New Zealandhads been reached the adequate level of protection till to 2013.[62] Thirdly, the evaluation of the level of data protection in third countries will induce tical tensions. The assessment of the protection level of personal data for the third country actually is the assessment of the protection level of fundamental human rights of the third country in the data protection field. Some countries will revolt the assessment on personal data protection level, which comes from the EU. In 2001, the Article 29 Working Party published the recommendation of Australia Privacy Act, and it introduced the conflict between Australia and the EU.[63]

2.3.2. Exemption Clause

Besides through the rules of "Adequate Level of Protection" to transfer the personal data cross-border, Article 26 Para. One of the Directive also set up a series of rules of exemption clause as the legal basis to transfer the personal data cross-border to the third county. However, it should be noted that these exceptions are based on the situations that the personal data transfer will only conduce small impact to the data subject, or that there are other rights and interest which take precedence over personal data. Therefore, these exceptions are extremely special that need to be taken narrow and rigorous interpretation.[64] There are six exemption clauses formulated under the Directive: a) Obtained the specific consent from the data subject; b) In order to perform the contract between the data subject and the controller; c) In order to conclude or perform a contract concluded in the interest of data subject between the controller and the third party; d) In order to protect the public interest or for the establishment, exercise or defence of the legal claim; e) In order to protect the vital interest of the data subject; f) the transfer is made from a register of public administration.

---

[62] European Commission, *2013/65/EU: Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand (notified under document C (2012) 9557) Text with EEA relevance*, *OJ* L 28, 30 January 2013, pp. 12–14.
[63] Kuner, Christopher. *European data protection law: corporate compliance and regulation*. Vol. 20. Oxford: Oxford University Press, 2007.
[64] Lynskey, Orla. *The foundations of EU data protection law*. Oxford University Press, 2015.

The “Consent of the data subject” is the most forceful instruments in the exemption clause to transfer the personal data cross-border. Therefore, this powerful instrument should be limited strictly, and the Article 29 Working Party deems that the “Consent of the data subject” is legal and enforceable that fulfil the four conditions. First, the contents and expression of consent must be unambiguous; Second, the consent must be made freely; Third, the content of the consent must be explicit; Fourth, the consent must be made with sufficient information. That means when the data subject of the EU clicks the “I accept” on the business website of a third country, if those standard clauses which should be accepted are cumbersome, ambiguous and hiding under those numerous web links, actually, before the data subject accept those clauses, they do not get the reasonable chances to check and understand those clauses. Therefore, clicking the “I accept” option is not made by the data subject with sufficient information, and such consent is considered invalid by the data protection agencies of the Member States.[65] Therefore, legal documents that require the consent of the data subject need to pay special attention to the use of the language, and cannot use a language which is ambiguous and hard to understand, because data subject cannot express consent according to a legal document written in a language that he cannot fully understand. Meanwhile, it should be noted that the consent of data subject is an exception to the cross-border transfer of personal data. The data protection agencies of the Member States have a very cautious attitude towards consent of data subject. For the companies that need to frequently transfer the personal data cross-border cannot rely on the consent of data subject in every time and cannot regard as that as general means to transfer.[66]

The exception of personal data cross-border transfer on “necessary for the performance of a contract between data subject and controller” must strictly limit the interpretation on the “necessary”. For example, a user in France through the internet services application to rent a vehicle for the travel in China, that the services provider needs to transfer the user’s information such like the personal information, contact information and credit information cross-border to China, this kind of transfer will be regarded as “necessary”. However, in the last example, if that services provider wants to collect the personal information of those users and build a database which located in China for the convenient on further business or distribute the advertisement, this

[65] Kuner, Christopher. *European data protection law: corporate compliance and regulation*. Vol. 20. Oxford: Oxford University Press, 2007.
[66] Poullet, Yves. "EU data protection policy. The Directive 95/46/EC: Ten years after." *Computer Law & Security Review*22.3 (2006): 206-217.

kind of condition are failed to fulfil the requirements of "necessary" for the performance of a contract because that is only helped for the performance of a contract, the services provider still could store those data in Europe. When the subject who need to transfer personal data cross-border through the "contract performance", they need to consider is that exist the high connection between the interest of data subject and contract performance. That the "contract performance" fails to implement in the personal data transborder flows if the data controller is just stating that personal data cross-border transfer could significantly reduce the cost of the corporation or for the business interest of the corporation.[67]

In order to protect the vital interests of data subject to process a necessary transfer of personal data, the implement requirements of this exception are really strict. It will only apply to the situation that the data subjects are unavailable to make a decision by themselves and assume if they could make a decision, they will definitely agree.[68] For example, if a Germany citizen, unfortunately, got a car accident and become unconscious at China, in this kind of condition, the data subject cannot make a consent to the transfer of his personal medical information. And then the controller of that patient's personal medical data could transfer those important data to the hospital in China immediately and without any other requirements.

The exception conditions that "transfer was made a register in public agency" also limited in a few types of data, because it required the all Member States already exist those public registration agencies, like business registration and land ownership registration.[69] Besides, this exception does not allow the company to transfer the entire database or a certain type of information in the database, but rather to transfer the personal data provided by the applicant to the enquiry when the public registration agency provides an inquiry to an applicant with legitimate interests.

All those six exception conditions of data transfer in the Directive are concern about protecting legitimate interests. In practical application, except for the "consent of data subject", the other types of exceptions are really rare. The exemption clause does not address the main contradiction between the protection of personal information and the cross-border transfer of personal information.

---

[67] Cate, Fred H. "The EU data protection directive, information privacy, and the public interest." *Iowa L. Rev.* 80 (1994): 431.
[68] Cate, Fred H. "The EU data protection directive, information privacy, and the public interest." *Iowa L. Rev.* 80 (1994): 431.
[69] Kuner, Christopher. *European data protection law: corporate compliance and regulation*. Vol. 20. Oxford: Oxford University Press, 2007.

2.3.3. The Standard Contractual Clauses (SCC)

In order to regulate the tremendous personal data transfer which cross-border, the Article 26, Para.2 also provide another condition, that is via the "Adequate Safeguards" to fulfil the requirements which equal with the requirements of "Adequate Level of Protection".[70] And Article 26, Para.4 authorised the Commission to formulate the contents of SCC, for the personal data cross-border transfer through the SCC will be regarded as already provided the adequate protection measures. That means the signed SCC is not only effective between the signing parties, but the Directive also gives the legal effect of the SCC. The EU also could transfer the personal data via the SCC model to those countries and regions which have not been assessed as "Adequate Level of Protection".

The SCC was started at 1992, at that time, the Council, the Commission and the International Chamber of Commerce have jointly approved a series of model contracts on personal data internationally transfer as the samples. However, those contracts are too broad to resolve the issues of Transborder Data Flows, and then the Commission has not officially approved those model contracts at last.[71] In 2001, after the publishing of the Directive, the Commission published two types of SCC, one is for the "controller to controller", and another is for the "controller to processor".[72] However, the business corporations are extremely unsatisfied on those two contracts because those contracts could not meet their needs at all. Finally, the main disputes have been resolved in 2004 and published a new contract to replace the old one which published in 2001. There are three SCC available at present and provide for the parties to choose freely, in this thesis will only introduce the most practice and most important one of them, the "controller to controller" which published at 2004 (Hereinafter referred to as "The 2004 Contract")[73].

The main clauses of the 2004 Contract are a) The obligations of the data exporter and data importer. The data

---

[70] Directive 95/46/EC, *OJ* L 281, 23 November 1995, Article 26 para.2.
[71] The Council, the Commission and the International Chamber of Commerce, "*Model contract to ensure equivalent protection in the context of transborder data flows with explanatory report (1992)*", Study made jointly by the Council of Europe, the Commission of the European Communities and International Chamber of Commerce (2 November 1992).
[72] European Commission, Standard contractual clauses for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to third countries which do not ensure an adequate level of protection (controller to controller (2001).
[73] European Commission, Commission Decision C (2004)5721 SET II Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers) (2004).

exporter should be compliance with the EU regulations and domestic law of Member States, on the collection, process, and transfer of personal data, besides, the data exporter needs to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under the clauses of the SCC. The obligations of data importer are purer. They need to take efforts on the data security at import county or region, protect the personal information of data subject. b) The clause of third-party beneficiary rights. In order to protect the data subject's personal information more effectively, the 2004 Contract established the data subject as the third party and establishing in the contract for the data subject almost all the data subjects have rights in the Directive like the data processing must get the explicit consent of the data subject, the right to require to delete the information, and rights to ratification, etc. c) The clause of the liability sharing. The Commission considers that the data subjects are easy to trace accountability to data exporters; thus, in the SCC, the data exporter were allocated more burdens then data importer. The 2004 Contract was on the basis of obligation allocation between the data exporter and the data importer, added the extra obligation, the "reasonable effort" to the data exporter. The Article 3 of the 2004 Contract, each party shall be liable to the other parties for damages it causes by any breach of these clauses; the data subject should ask the data exporter to take the measures to make to enforce his rights at first, if in a reasonable period the data exporter still has not taken such action, the data subject has the right to ask the data importer to take the remedies measures. That means the data exporter not only need to take themselves obligation under the contract but also need to take "reasonable efforts" to make sure the data importer also implementing their contractual obligations.

The SCC model was amplified the application scope of the Directive, the clause of the third-party beneficiaries' rights made the data subject got almost all the rights of the data subject, which regulated under the Directive, at the third country. And let the data importer in the third county, which has not reached the "adequate level of protection" also needs to be compliance with the requirements of the Directive to protect the personal data. However, the SCC still exist several defects, first, the core clause of the SCC, the clause of third party beneficiaries rights, whether it is established or not depends on the identification of the third party beneficiaries contract by the applicable law of the SCC.[74] The applicable law of the SCC is the domestic law of the data exporter's country, that is the contractual law of the Member States. However, the legal systems are different between the Member States, some jurisdiction would allow the breakthrough of the relatively of debt and sets

[74] Kuner, Christopher. *European data protection law: corporate compliance and regulation*. Vol. 20. Oxford: Oxford University Press, 2007.

the rights and claims for the third party, in other jurisdictions that are prohibited.[75] Since that, the SCC may not provide the legal basis for some countries to transfer the personal data cross-border. Second, the SCC cannot resolve the problem on the transfer the personal data in the internal circle of the multinational companies. The SCC requires the data exporter and data importer transfer the personal data cross-border based on the contract, that means different departments, different branch companies which in one multinational company, or the different office which belongs to one international law firm could not transfer the personal data cross-border under the SCC model because the same legal entity cannot sign a contract.[76] Besides, when the numerous and complex transfer on the personal data happens, that needs to signed hundreds even thousands of contracts, undoubtedly, that heavily burdens both for the data exporter and data importer.

2.3.4. The Binding Corporate Rules

The transborder data flows are inevitable for the multinational company on the business, not like the data transfer between the two independent companies, the data transfer in the internal of the multinational company, the data exporter and data importer do not have the ability to sign a contract under the legal context. Since that, the SCC seems not a wise choice for the multinational companies under this situation. Fortunately, the Article 29 Working Party published a series of legal documents to establish a brand-new tool which aims to fix this problem, the Binding Corporate Rules (BCRs).[77] The BCRs is designed for the multinational companies or multinational group enterprises, that are legally binding rules on the transfer and process data in an internal circle of a corporation or a company. The BCRs will be regarded as fulfilling the requirements of the "adequate safeguards" which lay down the Article 26, Para.2 of the Directive, and also be treated as an exception of the "adequate level of protection", all those measures let the BCRs become the forcible mean for the multination companies to transfer the personal data cross-border internally, and disregard whether the recipient's country

---

[75] Kuner, Christopher. "Regulation of transborder data flows under data protection and privacy law: past, present, and future." *TILT Law & Technology Working Paper* 016 (2010).
[76] Kong Lingjie, *Legal protection of personal data privacy*, Wuhan University Press, 2009.
[77] European Commission, Data Protection Working Party, WP 74: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, 3 June 2003; European Commission, Data Protection Working Party, WP107: Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules", 14 April 2005; European Commission, Data Protection Working Party, WP 108: Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, 14 April 2005; European Commission, Data Protection Working Party, WP 133: Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data, 10 January 2007; European Commission, Data Protection Working Party, WP 153: Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, 24 June 2008.

meets with the requirements of "adequate level of protection" or not.

2.3.4.1. The Application and Permission of the BCRs

Firstly, the BCRs needs to ensure who is the applicant, the duty of the applicant is to represent the multinational company to submit the application, and the company needs to ensure all the other legal entities of the company obey the BCRs, even those legal entities are not located in the Member States. If the headquarter of this company in the Europe Union, that the headquarter needs to be the applicant, otherwise, the company needs to designate a legal entity which in the European Union as the applicant.

Then, after the applicant submits the application, the applicant needs to choose a competent lead data protection authority (Lead DPA), for the convenience, it always let the data protection authority which located near form the applicant as the Lead DPA. After that, the applicant needs to follow the requirements of the Article 29 Working Party's legal documents to formulate the proposal of the BCRs and submit the proposal to the Lead DPA. The Lead DPA will assist the applicant in revising the BCRs proposal and referring the revised proposal to the others DPA of Member States to check and approve. The applicant needs to base on the feedback and suggestions of those DPA and make the last version of the BCRs, at last, after the confirmation of those DPA, the approved BCRs required to be filed at the Article 29 Working Party.[78]

2.3.4.2. The Contents of the BCRs

Every multinational companies' business models are totally different; even the different region office in one corporation also exists a huge gap in the functioning models. As a consequence, those difference will trigger difference between the rules on the data protection and data process, under this kind of situation, the Article 29 Working Party thought that is really hard to implement to all the multinational enterprises if the BCRs is similar with the SCC, which means all the multinational enterprises use the same standard contract. Since that, the Article 29 Working Party did not formulate the standard contents on the template of BCRs but required the

[78] European Commission, Data Protection Working Party, *WP107: Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules"*, 14 April 2005.

multinational enterprises' BCRs follow and obey the Directive and needs including those contents: a) The third-party beneficiaries clauses which similar with the SCC; b) The compensation and remedy when the multinational corporations violate the BCRs; c) The multinational corporations shall bear the burden of proof if the data subject and the multinational corporations are involving the data protection litigation; d) The multinational corporations shall establish internal audit system; e) The multinational corporations have an obligation to corporate with lead DPA. Besides, when the applicant is applying the BCRs, they should provide a description of how the BCRs constrain the members of the corporation and their employees, the certification that the corporation has enough assets, etc., those entity contents are tedious and complex.[79]

2.3.4.3. The implementation and supervision of the BCRs

The BCRs have a rigorous and well-defined implementation and supervision system. Firstly, the multinational corporation will via the internal training to make sure all the departments and employees well-understand the BCRs and implement the BCRs in the business. Then the multinational corporation shall appoint a special department or special staff to supervise the situation of the implementation and supervision of the BCRs in the multinational corporation. Secondly, the multinational corporation will regularly audit on the compliance with BCRs, and the transfer of personal information of enterprises is audited by external certified independent auditing institutions. Thirdly, the BCRs established a complaint processing mechanism for data subjects to ensure if the data subject's personal data has been infringed, their complaints and objections could be resolved timely. The data subject which been infringed could base on the BCRs to claim the compensation for their damage to the designated applicant within the EU, and the multinational corporation should make appropriate measures to ensure the applicant within the EU have sufficient compensation. Besides, the data subject has the right to sue in the court where the legal entity, which transferred the personal data, are located, or where the headquarters of a multinational corporation and the applicant are located. Fourthly, the multinational corporation should fulfil the obligations for corporate with the lead DPA and followed the recommendations of the lead DPA.[80]

---

[79] European Commission, Data Protection Working Party, *WP 153: Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*, 24 June 2008.
[80] Lingjie Kong, *The Legal Protection on Personal Private Information*, Wuhan University Press, 2009.

2.3.4.4. The Comments to the BCRs

The BCRs actually formed an internal "Safe Harbor" for the multinational corporation, the personal data could be transferred legally from one department of multinational corporation cross-border to another department, and those data will be protected in the same level whether where they are. It is really providing convenience for the multinational corporation's branch companies, subsidiaries, and departments which all over the world on personal data transformation. The BCRs via the internal rules of the multinational corporation to achieve the protection of the personal information, and it is built on the basis that the enterprises' self-regulation system and the administration of the government the complementary means. The BCRs reduced the heavy burdens of governmental data supervision agencies on the data section. The reason is that the BCRs transferred the responsibility of the supervision on the personal data cross-border flows from the government to the multinational corporation itself.[81] Besides, the multinational corporation also through the discipline of employee and the contract of employment those means to put the protection on the personal privacy and individual's rights in the fundamental norms of the whole group.

However, although the BCRs provide extremely convenient to the transborder data flow, meanwhile it also needs to face tremendous challenges. Firstly, the approval procedure of BCRs is complicated and uncertain, though the Article 29 Working Party published three legal documents to explain the details of the substantial requirements and approval procedure, the most contents of approval still decided by the lead DPA and the when the data protection agency in every Members States as the lead DPA, they still have a series rules on approval procedure which established by themselves. Secondly, the approval procedures are endless and expensive. According to the report of the BCRs by Allen & Overy, in general, the approval procedure needs to cost 12-24 months from initial filing to final validation, the fastest record of application which under the assist by Allen & Overy also costs 11 months.[82] Third, the early application work and post-maintenance costs are high. All those high costs made only several large multinational corporations could support. The BCRs seems not friendly to the SMEs. Until present, only 122 multinational corporations have been authorized to join in the BCRs, which include, Airbus, American Express, CISCO, e-Bay, Hermès, International Business Machines Corporation, PayPal, etc.[83]

---

[81] Moerel, Lokke. Binding corporate rules: corporate self-regulation of global data transfers. OUP Oxford, 2012.
[82] ALLEN, OVERY. "Binding Corporate Rules." May 2016, http://www.allenovery.com/SiteCollectionDocuments/BCRs.pdf .
[83] European Commission, "BCR overview until 25th May 2018." 25 May 2018, https://ec.europa.eu/info/law/law-topic/data-

2.3.5. The U.S. - EU Safe Harbor

In the legislation of personal data protection, the EU and the U.S. has a huge difference in purposes. The EU's legislation of personal data protection was leading by the fundamental human rights, which incorporated into Article 7 & 8 of the Fundamental Rights of the European Union.[84] Meanwhile, the EU via the Treaty of the European Union made binding all of the Member States.[85] Since that, the Directive is really strict on the Transborder Data Flows, especially when those data are sensitive the personal data which linked with the personal privacy, all those measures are aimed to protect the personal privacy and human rights. However, the United States' legislation on personal data protection was leading by the market and its self-regulation, it is largely industry-specific and various by sector[86] , and the US legal system treats privacy as a personal property right that may be disposed of as one sees best, rather than an unassailable human right[87]. For example, in the U.S. collecting and processing of personal data is legal unless it causes harm or is expressly limited by U.S. law,[88] by contrast, in the EU, processing of personal data is prohibited unless there is an explicit legal basis that is permitted.[89] That is obviously existing a gap between the EU's and the U.S.'s attitude towards personal data protection, and the EU and U.S. also admitted those difference.[90]

At that time, the 90s of last century, the EU and the U.S. still are two most powerful economic entities in the world, and there are the largest trade and investment partners for each other, in 1999 the U.S. had $350 billion in trade with the EU.[91] After the published of the Directive, the "Adequate Level of Protection" will exclusive those U.S. companies out of the "white list" of the transborder data flows, besides, the Article 26 of the Directive, the exemption clause, also could not provide the legal basis for those U.S. companies to transfer

---

protection/international-dimension-data-protection/binding-corporate-rules-bcr_en .

84 Treaty (EU) C 326/391, *Charter of Fundamental Rights of the European Union*, *OJ* C 326, 26 Oct 2012, available at: http://data.europa.eu/eli/treaty/char_2012/oj .

85 Treaty (EU) C 326/01, *Consolidated version of the Treaty on European Union*, *OJ* C 326, 26 Oct 2012, available at: http://data.europa.eu/eli/treaty/teu_2012/oj .

86 Weiss, Martin A., and Kristin Archick. "US-EU data privacy: from safe harbor to privacy shield." (2016).

87 Long, William J., and Marc Pang Quek. "Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise." *Journal of European Public Policy* 9.3 (2002): 325-344.

88 European Commission, Collecting & processing personal data: what is legal?, available at: http://ec.europa.eu/justice/data_protection/data-collection/legal/index_en.htm .

89 Tourkochoriti, Ioanna. "The Snowden revelations, the Transatlantic Trade and Investment Partnership and the divide between US-EU in data privacy protection." *University of Arkansas at Little Rock Law Review* 36 (2014): 161-176.

90 Assey Jr, James M., and Demetrios A. Eleftheriou. "The EU-US privacy safe harbor: smooth sailing or troubled waters." *CommLaw Conspectus* 9 (2001): 145.

91 Long, William J., and Marc Pang Quek. "Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise." *Journal of European Public Policy* 9.3 (2002): 325-344.

personal data cross-border.[92] Obviously, the Directive will be a tremendous obstacle for the business between the EU and the U.S., for instance, once the Directive in force, the U.S. companies could not transfer the EU consumers' information to the U.S. for the analysis, the medical agencies also could not transfer the EU patients' information to the U.S. for the research and study, and the U.S. multinational corporations could not transfer the EU employees' information to the U.S. headquarters. In order to address this issue, the Commission of the EU and the Department of Commerce of the U.S. started the official negotiation in 1997, with the help of the U.S. industry and one-half years negotiations, the first version proposal of Safe Harbor has been published in November 1998 and has been passed in May 2000 after two rounds revised.[93]

2.3.5.1. The Privacy Principles of Safe Harbor Framework

The Safe Harbor Framework is specially made for personal data cross-border transfer between the EU and the U.S. Actually, in essence, the "Safe Harbor Framework" seems like a special "Adequate Level of Protection" for the U.S.'s companies. The difference is that the "Adequate Level of Protection" is a "white list" for all of the legal entities in the country which has been affirmed reached the "Adequate Level of Protection", but the "Safe Harbor Framework" is a "white list" for the companies of the U.S. which joined this framework, that evaluates a company as a unit, not a country.[94] The Safe Harbor Framework allows the companies of the U.S. to self-regulation and self-certifies annually that they fulfil the requirements which, according to the Directive, it conclude seven privacy principles:

a) Notice, the information collector has an obligation to notify the individual that the purpose of they collect and use information, and they need to provide the information about how the individual can contact the collective with any inquiries and complaints when collector disclosure the information to the third-parties. That means the collector's rights has been limited on use and disclosure.
b) Choice, the collector must provide the chance to an individual to choose whether their personal information will be disclosed to third-party and be used under the initial purpose of collection or other incompatible purposes of collection. The individual could choose "opt-in" or "opt-out", the "opt-in"

[92] Long, William J., and Marc Pang Quek. "Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise." *Journal of European Public Policy* 9.3 (2002): 325-344.
[93] Bo Wang. "The Comments of the EU and the U.S 'Safe Harbor Framework' ." *Knowledge Economy* 4 (2013): 46-47.
[94] Assey Jr, James M., and Demetrios A. Eleftheriou. "The EU-US privacy safe harbor: smooth sailing or troubled waters." *CommLaw Conspectus* 9 (2001): 145.

means if haven't obtained the explicit permission of individual will be treated as disagree, the "opt-in" normally be used on the collection of sensitive personal information. The "opt-out" means if haven't obtained the explicit permission of the individual will be treated as agree, the "opt-out" normally be used on the collection of normal personal information.

c) Onward Transfer, the collectors, should apply the Notice and Choice principles when they disclose the personal information to the third-party and make sure the third party also joined the "Safe Harbor Framework" or is subject to the Directive or another adequacy finding. Besides, the collector also could through the contract to ask the third party to provide the same level of protection to personal information.

d) Access, the individual has the rights to correct, amend, or delete that information where it is inaccurate unless where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

e) Security, the collector must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

f) Data Integrity, the collection of information should have an explicit purpose and take reasonable measures to make sure that information is reliable for its intended use, accurate, complete, and current.

g) Enforcement, to ensure compliance with the Safe Harbor principles, there must be: 1. readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved, and damages awarded where the applicable law or private sector initiatives so provide; 2. procedures for verifying that the commitments companies make to adhere to the Safe Harbor principles have been implemented, and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self-certification letters will no longer appear in the list of participants.[95]

[95] Kuner, Christopher. *European data protection law: corporate compliance and regulation*. Vol. 20. Oxford: Oxford University Press, 2007.

2.3.5.2. The Comments of the "Safe Harbor Framework"

That is not hard to find out the structure and the characters of the "Safe Harbor Framework" through these seven Privacy Principles. Firstly, the core concern of the "Safe Harbor Framework" is privacy protection. In a way, the tasks of the "Safe Harbor Framework" is to fix the issues of the difference of privacy information protection system on the transborder data flows between the U.S. and the EU, so the "Safe Harbor Framework" spent lots of space to explain the obligations of the data collectors and the explicit rules of the data subjects' rights, besides, the "Safe Harbor Framework" also required the third-party also needs the requirements of "Adequate Level of Protection" or other conditions of the Directive. Secondly, the "Safe Harbor Framework" highly relies on the self-regulation of companies. The "Safe Harbor Framework" actually is a virtual community which just published several fundamental privacy protection principles, and any U.S. companies only need to declare they will obey the principles of the "Safe Harbor" and proposed a scheme about how to implement, at last, after official file and obtained the authorization of the Department of Commerce of the U.S., those companies could transfer the personal data from the EU to the physical territory of the U.S. legally. However, the privacy information protection in the procedures of processing after the transferred only could rely on the self-regulation of the company, the surveillance mechanism will be functioning and sue the company for commercial fraud if the official department finds the company is failed to fulfil the obligations.[96] Thirdly, the implementation of the "Safe Harbor" reflects the compromise between the U.S. and the EU. The "Safe Harbor" regulated three mechanisms to implementation, the compliant, the penalty, and the supervise. The compliant mechanism is operated independently by industry association, for companies that are not attributable to any organization or association, they must voluntarily accept cross-border investigation and supervision of private data protection agencies in the Member States.[97] The penalty includes retracting the certification, publishing the company's infringement until it is submitted to the Federal Trade Commission for further legal action. For the supervise, all the corporations whom cannot be supervised by the American's agencies under the law will be prohibited to join the "Safe Harbor", and that's required the U.S. government to take some enforcement actions and established the management mechanism to ensure the implementation of the "Safe Harbor Framework".

---

[96] Bo Wang. "The Comments of the EU and the U.S 'Safe Harbor Framework' ." *Knowledge Economy* 4 (2013): 46-47.
[97] Fang Ma. "The Existence and Abolition of the US-Europe Cross-Border Information 'Safe Harbor'." *China Information Security* 11 (2015): 106-109.

Through those basic outlines of the "Safe Harbor Framework", we could easily find out that the conceptions of the EU and U.S. on the personal privacy are totally different, the EU treats the personal privacy protection as the fundamental and unassailable human rights and the U.S. traditional concept treats the personal privacy as a personal property right.[98] Under those circumstances, we could undoubtedly say the "Safe Harbor Framework" is built on a huge compromise between the U.S. and the EU. Those two friends showed the most reliable faith to each other. However, it also becomes the Achilles' heel of the Safe Harbor.

2.3.5.3. The Collapse of the Safe Harbor Framework

At the beginning only a small number of organisations registered into the Safe Harbor, 400 companies until 2004, then the membership has gradually increased beyond 5000.[99] That seems the Safe Harbor was tracked into a right railway and keep going; however, the whole framework was collapsed by the *Schrems* case.[100]

In 2013, the biggest intelligence scandal of the U.S. in this century was broke out, the PRISM surveillance program, which disclosure by Edward Snowden, the former intelligence agent of U.S. National Security Agency (NSA). The NSA could surveillance all the information through the network that they can reach and even without the order of a court.[101] Under this kind of circumstance, on June 25, the Austrian citizens Maximillian Schrems made a complaint to the Irish Data Protection Commissioner that the Facebook-Ireland was infringing his personal data that transferred his personal data cross-border from Ireland the U.S. and without the permission of himself, those personal data was exposure and faced high risks under the PRISM program. Then the Irish DPA has dismissed the complaint and alleged that Facebook fully complied with the Safe Harbor and the Schrems have not submitted any evidence that could prove his data was being infringed.[102] Obviously, the Schrems would not accept this consequence, and he appealed this decision to the Irish High Court to initiated judicial review proceedings. Then, the High Court held that actually the Schrems has the

---

98 Long, William J., and Marc Pang Quek. "Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise." *Journal of European Public Policy* 9.3 (2002): 325-344.
99 European Commission, "The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce," *SEC* (2004) 1323, 20 Oct. 20, 2004.
100 Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015, ECLI:EU:C:2015:650, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 .
101 Greenwald, Glenn. *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. Macmillan, 2014.
102 Weiss, Martin A., and Kristin Archick. "US-EU data privacy: from safe harbor to privacy shield." (2016).

legal standing under the domestic and EU law to make this complaint, and the Safe Harbor Agreement which published in 2000 seems failed to compliant with the current EU data protection law that after the development of the Lisbon treaties which merged the Fundamental Rights into the EU law and entered into force on December 2009.[103] With all those questions, the High Court referred the matter to the ECJ.

On October 6, 2015, the ECJ released answers of the Irish High Court and declared the Safe Harbor Agreement violates the EU law and invalidated Safe Harbor immediately.[104] Under the principles of the Charter of Fundamental Rights of the European Union (The EU Charter)[105], such as the right to respect for private life (Article 7), right to protection of personal data (Article 8), right to an effective remedy (Article 47), and the Article 25 and 28 of Data Protection Directive, the national DPAs has an obligation to examine is the third countries or regions has the ability to provide the essentially equivalent protection for personal data and guaranteed the compatible with the EU law that the transborder data flow only will be permitted if the third county ensures an adequate level of data protection.[106] Obviously, the PRISM disclosure that the U.S. put the national security, public interest and law enforcement requirements, etc. in the primary protection objects and regardless any agreements or commitments, include the Safe Harbor principles.[107] Meanwhile, since the Safe Harbor Agreement was lack of an effective judicial remedy, the ECJ also held the Safe Harbor Agreement was incompatible with Article 47 of EU Charter.[108]

However, the Safe Harbor Framework was too politically and economically necessary, more than 5000 companies rely on this bridge to transfer the data between the U.S. and the EU, it is extremely important for both U.S. and the EU. In order to prevent economic catastrophe, the negotiations between two parties were immediately enacted after the ECJ issued the decision. Only four months after, on February 2, 2016, the Commission announced the "Privacy Shield"[109] would replace the "Safe Harbor". And two months after, the

---

[103] Ni Loideain, Nora. "The end of safe harbor: Implications for EU digital privacy and data protection law." *Journal of Internet Law* 19.8 (2016).
[104] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015, ECLI:EU:C:2015:650, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 .
[105] Charter (EU) C 326, *Charter of Fundamental Rights of the European Union*, *OJ* C 326, 26 Oct 2012, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT .
[106] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015, ECLI:EU:C:2015:650, para 66, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 .
[107] Ni Loideain, Nora. "The end of safe harbor: Implications for EU digital privacy and data protection law." *Journal of Internet Law* 19.8 (2016).
[108] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015, ECLI:EU:C:2015:650, para 66, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 .
[109] Decision (EU) 2016/1250, *pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, *OJ* L 207, 1 August 2016, p. 1–112, available at:

Parliament and the Council passed the GDPR, that embodies the legislation of personal data protection enters into a brand-new stage.

2.4. The Legislation Reform of Transborder Data Flows on Personal Information

2.4.1. The Background of the GDPR

Nowadays, the New era of digital technology was highly developed in the world, and it brings numerous new technologies like Cloud Computing, Blockchain, and Big Data. All those Internet Communication Technology also brings challenges to the legal system on data protection, especially when the main legal instrument, the Data Protection Directive, was published in last the century. Obviously, the value of personal information already beyond the information itself at present, it has been given highly business value by the market, and the transborder data flow on personal data adds the fresh blood to the multinational e-commerce to explore the overseas market. Those strict and complex rules of the transborder data flow on the personal data which regulated by the Directive cannot fulfil the requirements of the New digital era, and those complicated regulation systems become the tremendous hiders to the development of the multinational E-commerce and multinational company.[110] Under this kind of circumstances, the Commission published a report about the reform of the Directive on November 4, 2010, the "*A Comprehensive Approach on Personal Data Protection in the European Union*". The report proposes to simplify the rules of the transborder data flow on the personal data and expand the scope of application.[111] In 2016, the "*proposal of the General Data Protection Regulation*" has been approved and it will be in force on May 27, 2018, and replace the Directive formally. And the Snowden disclosure the PRISM surveillance program also ringing the alarm on the protection of personal data, with the *Schrems* case, the Safe Harbor Framework was collapsed, and the "Privacy Shield" replaced it in July 2016. The GDPR was born under such complex and sensitive circumstances.

---

http://data.europa.eu/eli/dec_impl/2016/1250/oj .

[110] Ahmed, Shahab. "A Discussion of Practical Steps to Harmonize Data Protection Rules Globally." *Available at SSRN 1966281*, (2011).

[111] Communication from the Commission. "A Comprehensive Approach on Personal Data Protection in the European Union." *COM (2010)* 609 (2010).

2.4.2. The Basic Trends of the Reforms

The protection of the transfer of the personal data cross-border is the important contents of the data protection, and it has been entwined with many elements like the guiding ideology, legislation, and problem-solving. With the reforms from the “Personal Data Protection Directive” to the “General Data Protection Regulations”, the personal data cross-border flow protection system has also undergone specific and obvious changes in the reform.

1) Keep the balance of the data subject’s right and free flows of data

Since the Directive was published at the age that the internet still stays on the old stage, the information distributes and transfer point-to-point. And the objectives of the legislation on the Directive still stays on the protect the rights of the personal data subject which based on the computer automatically process the personal data.[112] And following the development and implementation of the Internet and Communication Technology, the data gradually out of the data subject’s control, and that will trigger numerous risks in those data subject’s digital life[113], even in the real world, besides, the transborder data flows were also highly connected with the business operation. In order to address the issues that protect the rights of personal data subject effectively and avoid setting various restrictions on transborder data flows, the revolution of from the Directive to the GDPR is more sophisticated and targeted, the purposes are more clarity, the contents are more affluent, and striving to find a balance in the free flows and effective protection on the personal data.

2) From the “Directive” to the “Regulation”

As the vital parts of the personal data protection system, the protection of the personal data on the transborder data flows also builds on the unified and coherent judicial system. Actually, in the legislation model of the EU, the directives are different with the regulations in the implementation and enforcement, the regulations only required the approved of the Commission, the Council and the Parliament and after the published by the Commission, the regulations will in force in every Member States. However, the directives demand the

---

[112] Kuner, Christopher. "Regulation of transborder data flows under data protection and privacy law: past, present, and future." *TILT Law & Technology Working Paper* 016 (2010).

[113] Introna, Lucas D. "Privacy and the computer: why we need privacy in the information society." *Metaphilosophy* 28.3 (1997): 259-275.

Member States transform it to the domestic law or regulation and to implement at the domestic level.[114] As a consequence, in order to promote the hierarchy of legislation this time, the EU adopts the "regulation" to support the reform of the personal data protection system. Through the "regulation" to avoid the difference in the legislation of the Member States which caused by the difference protection level, and to achieve unification on the legislation between the Member States.

3) The extraterritorial applicability has been enhanced

The implementation scope of the Directive only regulates the data controller and their activities which in the border of the Member States and for the purposes of personal processing data and the functioning devices are situated in Member States' territory[115]. Indeed, that is too narrow to protect personal information on the worldwide website nowadays. The territorial scope (Article 3 of the GDPR) stipulated that the regulation applies to the data controller and data processor established in the EU and regardless of whether processing taking out of the territory of the EU.[116] That is a huge step forward from the Directive, and it means the jurisdiction of the EU is no-longer restricted by the physic territorial border, any data processing activities which linked with EU citizens will be regulated by the GDPR. The territorial scope of the GDPR is broader than the Directive, and it also corresponds with the requirements of the personal data protection system on the transborder data flows.

2.4.3. The Adjustment on the Mechanism of Personal Data Cross-Border Transfer

The GDPR has not abandoned the mechanism on the personal data transborder flows established by the Directive, and the whole systems were remained and be improved through clarifying the standard and conditions for the transfer, especially on the definition of the "Adequate level of protection". The notion of "Adequate level of protection" in the Directive was always being blamed because it is ambiguous and

---

114 Chalmers, Damian, Gareth Davies, and Giorgio Monti. *European union law*. Cambridge university press, 2019.

115 Directive 95/46/EC, *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*, *OJ* L 281, 23 November 1995, Article 4 National law applicable, available at: http://data.europa.eu/eli/dir/1995/46/oj .

116 Regulation (EU) 2016/679, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*, *OJ* L 119, 4 May 2016, Article 3 Territorial scope, available at: http://data.europa.eu/eli/reg/2016/679/2016-05-04 .

vagueness.[117]

1) Clarify the standard and the condition of implementation of the "Adequate level of protection."

As the fundamental principles of the personal data transborder flows, the third county or organisation reached the standard of the "Adequate level of protection" is the precondition of personal data transfer.[118] First of all, the Commission recognized all former decisions on the assessment of the adequate level of protection, those countries and organisations will not be eliminated from the "White List" but still needs to obey the new rules under the GDPR.[119] On the basis of the evaluation procedure established by the Directive, the GDPR has clarified the specific elements when the Commission evaluates the third country or organisation. Article 45 paragraph 2 of the GDPR listed several elements of assessment, like the rule of law, human rights and fundamental freedom, public security and criminal law, etc.[120] And this article also required the third country to have at least one independent supervisory authority and committed take the responsibility from the legally binding convention.[121] The Commission also needs to assess the protection level according to the one or series data transfer, especially focus on the classes of the data, the purpose and duration of the data process, the imported state and exported state, etc., all those details on the personal data transfer.[122] Besides, since the GDPR adopts an open-listed legislative approach to the substantive criteria for decisions on adequacy level of protection, the Commission has a massive discretion right on the assessment that could be a "political bargaining chip" for the negotiations or exchange interests between the EU and other countries.[123]

2) The improvement on the SCC and the BCRs

The specific contents and operating mechanism of the Standard Contract Clause (SCC) and the Binding Corporate Rules (BCRs) already been analysed as above, those mechanisms are basic routes to transfer personal data cross-border and the GDPR has not made the substantial revise on them, only reinforce and improve some details.

---

117 Ni Loideain, Nora. "The end of safe harbor: Implications for EU digital privacy and data protection law." *Journal of Internet Law* 19.8 (2016).
118 Roth, Paul. "Adequate Level of Data Protection in Third Countries Post-Schrems and under the General Data Protection Regulation." *JL Inf. & Sci.* 25 (2017): 49.
119 Regulation (EU) 2016/679, *GDPR*, *OJ* L 119, 4 May 2016, Article 45 paragraph 4.
120 Regulation (EU) 2016/679, *GDPR*, *OJ* L 119, 4 May 2016, Article 45 paragraph 2.
121 Regulation (EU) 2016/679, *GDPR*, *OJ* L 119, 4 May 2016, Article 45 paragraph 2, (b)&(c).
122 Wagner, Julian. "The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?." *International Data Privacy Law* (2018).
123 Jin, Jing. "An Overview of the General Data Protection Regulation-Evolution, Key Points and Major Issues" *Chinese Journal of European Studies* 4 (2018): 1.

Firstly, the GDPR formally and legally take the BCRs in the regulation. In the former routes of the personal data cross-border transfer in the Directive, the BCRs have not been listed, it is created by the Article 29 Working Party and recommended this tool for the multinational corporations, and that caused the confusion on the legal status of the BCRs. In Article 47 of the GDPR, the BCRs have been formally recognized and clarified the specific contents of the BCRs which include the classes of personal data, the principles of protection, the responsibility of the corporates, the procedures of redress and the requirements of supervision.[124] Secondly, the Article 42 of GDPR established the data protection certification mechanism and the data protection seals and marks, and the new mechanism also provides convenience for the corporates which through the SCC or BCRs to transfer personal data cross-border.[125] The data protection certification mechanism is made to certificate the data controller, or data processor has reached and fulfilled the requirements of several special measures when they charge the personal data, and the companies that registered the certification could prove the legality and authenticity of their data protection to a certain extent, therefore, that could simplify the strict and tedious approval procedures of BCRs and SCC, improve the efficiency to both corporates and supervision departments.[126]

3) Expand the routes of personal data cross-border transfer

The GDPR expanded the routes of personal data transborder flows based on the Directive to meet the requirements of the reforms which caused by Internet and Communication Technology. The first adjustment is aimed at the situation that transfers personal data cross-border to the third country which did not reach the "adequate level of protection", the Article 46 of the GDPR revised the Article 26 of the Directive that if the data controllers and data processors could provide the "Appropriate Safeguard" on personal data protection and "Effective Legal Remedies" to the data subjects, they still could transfer personal data cross-border even the third county have not been listed in the "White List".[127] This measure provides an available path for those countries waiting for the Commission's assessment on the adequate level of protection, and the corporates that could offer appropriate surroundings for personal data but the local states haven't reached the requirements of

[124] Regulation (EU) 2016/679, *GDPR*, *OJ* L 119, 4 May 2016, Article 47.
[125] Regulation (EU) 2016/679, *GDPR*, *OJ* L 119, 4 May 2016, Article 42.
[126] Kamara, Irene, and Paul De Hert. "Data protection certification in the EU: Possibilities, actors and building blocks in a reformed landscape." *Privacy and data protection seals*. TMC Asser Press, The Hague, 2018. 7-34.
[127] Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 46.

the adequate level of protection.[128] The secondly is the GDPR amplified the contents of the clauses of "Specific Situation", for example, the Article 49 paragraph1(a) of GDPR introduced the "Data subject's consent" as the legal basis for the personal data transfer to the third country which cannot provide adequate protection and appropriate safeguard.[129] And that only requires explicit, specific and unbidden consent from the data subject as the precondition. This clause not only shows respect to the subject's willing but also provide an exception situation for the personal data cross-border transfer. Moreover, Article 49 also provides the other specific situation as the exception for the transborder personal data flows, such as pre-contract obligation, the necessary for the public interest, the necessity of the legal claim and protect the vital interest of the data subject. All those adjustments improved the flexibility and effectiveness of transborder data flows.

2.4.4. Enhanced the Supervision on the Transborder Personal Data Flows

Indeed, in the former supervisory mechanism on the transborder personal data flows that established by the Directive exist the issues on the effectiveness and the efficiency, and it caused the vulnerability on the personal data protection.[130] In order to fix those problems, the GDPR enhanced the obligations and duties of the data controller and data processor, proposed a series restrict requirements on them, and strengthen the supervision on the personal data transborder flows.

1) Strengthen the cooperation and the consistency of the supervisory authorities

For the effective and efficient supervisory system on personal data protection, and the cooperation and the consistency of the supervisory authorities, the GDPR established a new supervisory authority and explicitly declared its power, duties, and obligations. The Article 68 of the GDPR established the European Data Protection Board (EDPB) as the supervisory authority on the EU level to replace the Article 29 Working Party and is composed by the representatives of respective Member States' supervisory authority.[131] The new main tasks of the EDPB include, a) ensure the consistent application of the GDPR and supervise the application in every Member States; b) according to the requirements of the Commission, propose the advice, opinions, and

---

[128] Jin, Jing. "An Overview of the General Data Protection Regulation-Evolution, Key Points and Major Issues" *Chinese Journal of European Studies* 4 (2018): 1.
[129] Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 49 paragraph 1 (a).
[130] Fang Ma. "The Existence and Abolition of the US-Europe Cross-Border Information 'Safe Harbor'." *China Information Security* 11 (2015): 106-109.
[131] Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 68.

recommendations to the Commission when they formulate the legal documents on the data protection; c) draw up an annual report on the data protection of the natural person, and transmitted the report to the European Parliament, the Council and the Commission; d) offer professional opinions and recommendations to the Members States when the domestic data protection problems have occurred.[132] Besides, the EDPB also shall examine and approve the codes of conduct and binding corporate rules, assess the data protection level of the countries or organisations which as the data importers, that also is the tasks of the Article 29 Working Party used to be.

Same as the Directive, the GDPR also set up the rules on the supervisory authorities in the Member States that each Member States shall provide at least one independent public authority to be responsible for monitoring the application of the GDPR.[133] The difference is the GDPR made an explicit rule that the supervisory authorities in the Member States need to designate a representative to the EDPB. Therefore, this measure provides strong support to the cooperation and the consistency on the application of the GDPR.

Besides, the GDPR regulated each supervisory authority shall have the investigative powers, corrective powers, and authorisation and advisory powers.[134] The investigative powers include ordering the controller and the processor to provide relevant information, and through launch a data protection audit to investigate the servers and relevant devices of the controller and the processor.[135] The corrective powers empowered the authorities to issue warnings, issue reprimands, impose a temporary or definitive limitation, order the rectification or erasure of personal data, withdraw a certification, and impose an administrative fine pursuant.[136] And the authorisation and advisory powers include the issue the opinion about the personal data protection to the national parliament and government of Member States, and take legal action against infringement of data controllers and processors or participate in other legal procedures, etc.[137]

2) Improvement of the supervisory measures

The Directive focus on the prior permission and supervision but lack of the effective supervision after personal

---

[132] Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 70&71.
[133] Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 51.
[134] Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 58.
[135] Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 58 paragraph 1.
[136] Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 58 paragraph 2.
[137] Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 58 paragraph 3.

data has been transferred, and the GDPR initiate several measures to improve the effective supervision and protection surrounding for the personal data cross-border flows.

Firstly, the GDPR established the "Data Protection Officer" in the EU level to ensure the effective application of the GDPR on the data protection and cross-border data flows. The data controller and the data processor are the public authority or body, and the core activities are data processing operations, or the core activities of the data controller and the data processor are processing sensitive personal data, they shall designate a data protection officer that shall have the professional abilities on the data protection.[138] The main tasks of the data protection officer include: a) to inform and guide the data controller and the data processor; b) ensure the entities compliance with the GDPR and the domestic laws relevant with the data protection; c) cooperate with the supervisory authority; d) assist the data controller, and data processor communicates with the supervisory authority on the legal consultation.[139] The "data protection officer" actually is an internal supervisory mechanism for the legal entities, and this mechanism also built a bridge between the supervisory authorities with the data controller and the data processor, support the effective functioning of supervisory mechanisms on personal data protection.[140]

Secondly, the GDPR established the "Certification Mechanism" for the supervision of the data controller and data processor, and they could through registered the certificate to prove the legitimacy, authenticity, and advanced position of their works on the data protection, therefore, the certification mechanism could encourage the data controllers and data processors to compliance with GDPR to reach the certification. The certification mechanism facilitates the consistent implementation of data protection and high standards of data protection requirements.[141] The certification bodies were authorised by the domestic supervisory authority of the Member States or the national accreditation body.[142] The certification bodies shall keep the independence and without any interest or conflict with the data controller and data processor because the certification bodies' main tasks are issued the certification and withdraw the certification. The certification mechanism is complementary for the "adequate level of protection" on the personal data transborder flows,

---

[138] Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 37 paragraph 1.
[139] Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 38.
[140] Recio, Miguel. "Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability." *Eur. Data Prot. L. Rev.* 3 (2017): 114.
[141] Kamara, Irene, and Paul De Hert. "Data protection certification in the EU: Possibilities, actors and building blocks in a reformed landscape." *Privacy and data protection seals*. TMC Asser Press, The Hague, 2018. 7-34.
[142] Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 43.

and the certification mechanism is more flexible, convenient and friendly for the SMEs, the assessed procedures of the adequate level of protection are a heavy burden for those corporations because it is really expensive and complicated.[143]

Thirdly, the "adequate level of protection" also needs to be monitoring under the supervisory mechanism. The Commission should take responsibility for the persistently supervise the countries and organisations which in the "white list of the adequate level of protection".[144] For ensure the "adequate level of protection" are effective functioning to protect personal data, the Commission shall initiate a periodic review on the data protection circumstances of those countries and organisations and "eliminate" the countries or organisations from the white list timely when they failed to provide an adequate level of protection on the personal data.[145]

2.4.5. The Improvement of the Rights of the Data Subject

The reforms on the rights of the data subject are undoubtedly the core content of the GDPR and also is the biggest breakthrough from the Directive. The rights of the data subject are the basis of the personal data protection system, and the data protection system is the basis of the protection on the personal data transborder flows. Therefore, the improvement of the data subject's rights certainly will reflect on the protection of the personal data transborder flows. On the basis of the Directive, the GDPR added several rights of the data subject, the right to rectification, the right to erasure (Right to be forgotten), the right to restriction of processing, the right to data portability, etc.[146]

1) The right to rectification and the right to erasure (Right to be forgotten)

The authenticity and validity of personal data is the basis for the business on the personal data, the veracious personal data could lead the orientation for business to make the profit, and the correct personal data also could avoid the risk to the data subject because if the data was inaccurate, incomplete, or illegal, the data processing might cause disadvantage influence to the data subject. Hence, the GDPR set up the rights to ratification and

---

143 Kuner, Christopher. *European data protection law: corporate compliance and regulation*. Vol. 20. Oxford: Oxford University Press, 2007.
144 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 45 paragraph 4.
145 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 45 paragraph 3&5.
146 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Chapter 3 "Rights of the data subject".

the rights to erasure (Right to be forgotten) for the data subject.

The right to rectification ensures the data subject has the right to request the data controller to rectify the inaccurate personal data immediately and taking into account the purposes of the processing, the data subject also could require the data processes to complete the incomplete personal data.[147] And should be mentioned is the right to rectification is a kind of right of claim, that means the data controller and data processor were not must have to rectify the personal data when data subject claimed, whether rectify or not is depends on the specific situation.[148]

The right to erasure (Right to be forgotten) is the data subject has the right to ask the data controller to erase his or her personal data, and under several conditions, the data controller has an obligation to erase those personal data immediately.[149] Those specific conditions include a) the purposes of collection and processing no longer exist; b) the data subject's consent has been withdrawing; c) the objection of the data subject on the processing; d) illegal processing on the personal data; e) compliance with laws; f) information society services for the child.[150] And the data controller's obligation of erasure is independent, which means when those specific conditions happened, the data controller has to erase those personal data immediately even without the request from the data subject.[151] That also shows "the right to erasure (Right to be forgotten)" is a right of the formation; it is different from the right to rectification. Moreover, the GDPR also set up the restriction on the data subject to use the right to erasure, and the data subject could not initiate the right to erasure under the situations like, for exercising the right of freedom of expression and information; for the public interest; for compliance with a legal obligation; for media purposes or public health; for scientific research anhistoricalic research; for statistics and filing; for litigation, etc.[152] The core of the right to erasure (Right to be forgotten) is to ensure the data controller and the third parties could not access, read, and process those personal data anymore, that needs the data controller to make an effort to erase the links, the copies, and the replications of those personal data and inform the third parties take the same actions.[153]

---

147 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 16.
148 Jin, Jing. "An Overview of the General Data Protection Regulation-Evolution, Key Points and Major Issues" *Chinese Journal of European Studies* 4 (2018): 1.
149 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 17 paragraph 1.
150 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 17 paragraph 1, (a)-(f).
151 Jin, Jing. "An Overview of the General Data Protection Regulation-Evolution, Key Points and Major Issues" *Chinese Journal of European Studies* 4 (2018): 1.
152 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 17 paragraph 3.
153 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 17 paragraph 2.

2) The right to restriction of processing

The right to restriction of processing is designed to prevent the abuse of personal data, and the data subject has the right to restrict the data processing of data controller under several conditions when data subject contest the accuracy of personal data; or the processing is illegal, and the data subject opposes the erasure of the personal data, or for the data subject's legal claim; or the data subject exercise the right to object.[154] The data subject could exercise the right to restriction of processing to frozen the personal data to prohibit the data controller's processing, unless the data controller obtained the consent from the data subject, or for the initiate litigation; or for the protection on the rights of the natural person or legal person; or for the protection of public interest.[155]

3) The right to data portability

The right to data portability is an innovation of the GDPR, which aims to balance the free flows of personal data and the supervision on the personal data, let data subject could transfer data in a concise manner and also take control of they own data well.[156] The portability is the core of data to move, copy, or transfer, and this mechanism is key in promoting competition between the service providers and preventing lock-in effects.[157] Normally, the personal data was stored in the servers of the data controller, which means those personal data might be the private property of the data controller if they hold full control of those personal data, it will cause disadvantages the protection of personal data. And on the other hand, the personal data under the full control of the sole data controller also is an obstacle for the free flows of personal data.[158] The right to data portability means when data controller processing the personal data from the data subject, the data subject has the right to require the data controller to provide a copy of those data and without any restriction on further exercise and transfer.[159] And the data controller should provide the personal data in a structured, commonly used and machine-readable format and the data subject has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, and the data subject have the

---

154 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 18 paragraph 1.
155 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 18 paragraph 2.
156 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Recital 68.
157 Commission Staff Working Document, "On the Free Flow of Data and Emerging Issues of the European Data Economy", *Accompanying the Document Communication Building a European Data Economy*, 10.01.2017, SWD (2017) 2 final.
158 De Hert, Paul, et al. "The right to data portability in the GDPR: Towards user-centric interoperability of digital services." *Computer Law & Security Review* 34.2 (2018): 193-203.
159 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 20.

right to have the personal data transmitted directly from one controller to another, where technically feasible. Meanwhile, the GDPR also set up the restriction on the right to data portability that it could not be applied when the data processing actions under the requirement of public interest or official authority[160], and the exercise of the right to data portability take precedence over the right to erasure, which means the exercise of the right to data portability cannot interfere the third parties' fundamental rights and freedom.[161]

2.4.6. The Improvement of the Remedies and Penalties

In the past, the articles of the Directive about the specific legal remedies for the data subject and penalties for the infringers are ambiguous and endow the legislative power on details to the Member States. On the one hand, it causes a huge difference in the mechanism of data protection, remedies, and penalties between each Member States, on the other hand, it also influenced the consistent implementation of the remedies and penalties.[162] Therefore, the GDPR setup amount of provisions on the remedies and penalties based on the framework of the Directive to consistently apply in every Member States and ensure the achievement of the enforcement of remedies and penalties.[163]

Firstly, the GDPR gives two remedy options to the data subject when their rights have been infringed, the administrative or judicial remedy. If the data subject thought the processing of their data was inviolate the rules of the GDPR, they have the right to lodge a complaint to a supervisory authority, and the supervisory authority should inform the complainant on the progress and the outcome of the complaint.[164] Besides, the data subject also has the right to initiate a judicial remedy against the supervisory authority, or against the data controller or data processor.[165]

Secondly, the representation of data subjects. Article 80 of the GDPR regulated that data subjects have the right to mandate an organisation or an association to represent themselves to looking for a judicial or

---

160 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 20 paragraph 3.
161 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 20 paragraph 4.
162 Kuner, Christopher. *European data protection law: corporate compliance and regulation*. Vol. 20. Oxford: Oxford University Press, 2007.
163 Wachter, Sandra. "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR." *Computer law & security review* 34.3 (2018): 436-449.
164 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 77.
165 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 78&79.

administrative remedy. Meanwhile, those public interest organisation has the rights to complain to a supervisory authority if they consider the data subject's rights have been infringed and even without a mandate of the data subject.[166]

Thirdly, the highest administrative fine in the history of the legislation on data protection.[167] The person who has suffered damage as a result of an infringement of the GDPR has the right to receive compensation from the infringer according to Article 82.[168] Besides, in order to increase the burdens and costs of the infringement of the data controller and data processor, the GDPR set up a mechanism on the administrative fines. The supervisory authority could according to the Article 83 take two levels of administrative fines for different infringements, and the first level will up to 10 million EUR or the 2% of the total worldwide annual turnover of the preceding financial year, the second level will up to 20 million EUR or the 4% of the total worldwide annual turnover of the preceding financial year.[169] And the GDPR also empowered the Member States could take the administrative penalties in other forms as long as to ensure the appropriate, efficient, and cautiously.

2.4.7. The Privacy Shield Framework

After the *Schrems case* ended up the Safe Harbor Framework between the U.S. and the EU, the Commission and the Secretary of Commerce of the U.S. immediately initiate a discussion about the proposal a new agreement to replace the Safe Harbor, on February 29, 2016, the Commission officials released the Privacy Shield Agreement.[170] As the replacement of the Safe Harbor agreement, the Privacy Shield take a step forward on the clarify the responsibility and liability of the data controller and data processor and enhanced the legal remedies and penalties. However, the fundamental principles and the functioning mechanism of those two agreements are the same, the Privacy Shield framework also takes the voluntary entry mechanism and relies on the self-regulation and self-certification of the corporations, and the privacy principles also same with the Safe Harbor.[171]

---

166 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 80.
167 Kuner, Christopher. *European data protection law: corporate compliance and regulation*. Vol. 20. Oxford: Oxford
168 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 82.
169 Regulation (EU) 2016/679, GDPR, *OJ* L 119, 4 May 2016, Article 83.
170 Decision (EU) 2016/1250, *pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, *OJ* L 207, 1 Aug 2016, p. 1–112, available at: http://data.europa.eu/eli/dec_impl/2016/1250/oj .
171 Weiss, Martin A., and Kristin Archick. "US-EU data privacy: from safe harbor to privacy shield." (2016).

The following are the main difference between the Privacy Shield and the Safe Harbor: a) enhanced the administrative measures and clarified the liabilities of the data controller and data processor. For example, the corporation that left the Privacy Shield framework still needs to fulfil the requirements of the data protection in the Privacy Shield agreement if they choose to hold those personal data.[172] And the corporations should ensure the third-party, who received the personal data, also needs to provide an equal level of protection on the personal data. Meanwhile, the corporations should take responsibilities when third-party violated the Privacy Shield agreement. b) on the supervisory mechanism, the Privacy Shield not only regulate the restrict penalties but also introduce regular censorship, the Department of Commerce of the U.S. should take regularly investigate to the corporations in the Privacy Shield List, and the corporation persistently failed to comply with the principles of Privacy Shield agreement will be removed from the list. c) the Privacy Shield requires each corporation in the list should designate a privacy officer, the privacy officer should be independent with the national security authority and responsible for the provide the redress to the EU data subject. d) provide the multiple redress measures for the data subject which include, complaints to the corporation directly, and the corporation should reply in 45 days; take a complaint to the national data protection authority; mandate the public interest organisation to represent data subject, etc.[173]

Actually, the core values of the Privacy Shield are the same as the Safe Harbor, and the Privacy Shield agreement has been concluded not only means the rebalance between the personal data protection and personal data free flows between the U.S. and EU, but also signified compromise between the U.S. and the EU.

[172] Decision (EU) 2016/1250, *EU-U.S. Privacy Shield*, *OJ* L 207, 1 Aug 2016, paragraph 30-37.
[173] Voss, W. Gregory. "The Future of Transatlantic Data Flows: Privacy Shield or Bust?." *Journal of Internet Law* 19.11 (2016): 1.

3. Chapter Three: The Legislation of Transborder Data Flows of Personal Information in the United States, China and APEC

3.1. The Legal Framework of Protection of Personal Data Transborder Flows in the United States

The United States does not have an entire federal law on the protection of personal data transborder flows, and the United States has adopted decentralized legislation to protect personal data and citizens' privacy rights, it is different with the unified legislation of the EU. Meanwhile, the United States Federal Trade Commission (FTC) is responsible for data security of corporations and protection of citizens' privacy and promotes the legislation on the protection of personal data transborder flow through effective and efficient enforcement. Therefore, those separated legal instruments formed the United States' legal framework of personal privacy protection.

3.1.1. The Early Legislation of Privacy Protection in the United States

The privacy right is firstly reflected in the "*Fourth Amendment of the Constitution*" of the United States; its alleged citizens have the right to against unreasonable searches and seizures and protect themselves and their properties.[174] In 1974, the Watergate scandal was exposed that the federal agency's illegal surveillance and investigation on the individuals and frequently used and store personal information, in order to fix this public crisis and keep a balance between the administration of personal information and protection on citizen's rights, the U.S. passed the "*Privacy Act*".[175] The Privacy Act protects the records of individuals stored in the federal government system, and through detailed regulations to regulate the actions of federal agencies to collect personal data and stored. But the Privacy Act could not provide full and comprehensive protection on the

[174] U.S. Congress, *The first 10 amendments form the Bill of Rights*, Dec 15, 1791.
[175] The Act of United State, *Privacy Act of 1974*, 5 U.S.C. § 552a.

citizen's privacy rights, because the Privacy Act only applies to the federal level of the U.S. and exist many restrictions on the subject.[176] In 1986, the Congress of the U.S. published the "*Electronic Communications Privacy Act (ECPA)*"[177], the second chapter of the ECPA regulated the data transfer through electronic transmission, although the ECPA is aimed to protect personal privacy rights it still allows the FBI to issue survey letters to network service providers, asking them to provide information about respondents.[178] In 1988, the Privacy Act was being amended through the publication of the "*Computer Matching and Privacy Protection Act*"[179], it solved the problem of user information record in the automatic matching program. Except for the privacy protection legislation on the electronic information technology, the U.S. also expand it in another field, for example, the U.S. passed the "*Right to Financial Privacy Act (RFPA)*"[180] to regulate the recording of user information obtained by bank staff. In 1997, the White House formulated the "*A framework for global electronic commerce*"[181] to establish global guidelines of governance on the cross-border data transfer, and the legal basis of the transborder data flows of the U.S., the White House also requested the Department of Commerce to develop a unified international commercial legal framework to recognise, promote and facilitate electronic transactions worldwide, and work with the domestic private sector to establish domestic cyber privacy standards.[182] Then, with the development of Internet Communication Technology, the privacy protections in the U.S. was into a new stage, the age of big data.

3.1.2. The New Development of Privacy Protection in the United States

With the development of big data, the former protection framework of citizens' privacy has been impacted by the benefits brought by the cross-border data flows. Although big data has changed the world, it has not changed Americans' strong belief in protecting citizens' privacy, ensuring fairness, or preventing discrimination.[183] In 2014, the White House released the "*Big Data: Seizing Opportunities, Preserving*

---

[176] Annas, George J., Leonard H. Glantz, and Patricia A. Roche. "Drafting the Genetic Privacy Act: science, policy, and practical considerations." *The Journal of Law, Medicine & Ethics* 23.4 (1995): 360-366.
[177] The Act of United State, *Electronic Communications Privacy Act of 1986 (ECPA)*, 18 U.S.C. §§ 2510-2523.
[178] Mulligan, Deirdre K. "Reasonable expectations in electronic communications: A critical perspective on the Electronic Communications Privacy Act." *Geo. Wash. L. Rev.* 72 (2003): 1557.
[179] The Act of United State, *The Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507 (1988), amended the Privacy Act of 1974*, 5 U.S.C. § 552a.
[180] The Act of United State, *Right to Financial Privacy Act*, 12 U.S.C. §§ 3401-342.
[181] United States. White House Office. *A framework for global electronic commerce*. White House, 1997.
[182] Zhang, Sheng, "The International Law Regulation Path of Cross-border Data Flows by the United States and China's Countermeasures", *Business and Economic Law Review* (04)2019, pp.79-93.
[183] Choma, Alicja. "3.6. Big data–conditions of use and impact on business and society." *Quality. Central and Eastern Europe Focus*: 213.

Values"[184] to analyse the relations between the data economy and privacy protection and expect through revised the present policies and regulations to resolve the privacy protection issues. In 2017, the United States Federal Trade Commission (FTC) released the "Privacy & Data Security (2017)".[185] The report states that FTC creates a good environment for privacy protection and data security for cross-border data flows. The report also listed ten privacy cases and 4 data security cases that violated the FTC directives for the corporations to self-examine their mechanism on the protection of data transfer.

On March 24, 2018, the "*Clarifying Lawful Overseas Use of Data (CLOUD) Act"*[186] has been published, the first main part of CLOUD act is from the perspective of U.S. law enforcement agencies in obtaining evidence from foreign countries, it alleged the right to request for extraterritorial data should be based on the data controller rather than the data storage location, as long as the data is in the control of the U.S. service provider, the service provider is obliged to comply with the law in the United States. The second main part is the foreign law enforcement agencies take the data investigation in the U.S., that require to fulfil several conditions and provide the qualification of government. The CLOUD Act is the most important legal instrument on the cross-border data transfer in nearly a few years. The core value of the CLOUD Act is around the United States' interest that the law enforcement agencies have the right to request the data controller and data processor provide the data and no matter where the data been stored. And the CLOUD Act also supports the data free flows worldwide and against the data localization.[187]

3.1.3. The General Patterns of Protecting Transborder Personal Data Flows in the U.S.

As on above, we already mentioned the differences between the U.S. and the EU on the protection of the personal data transborder flows, and those differences also reflect on the general patterns of protecting the cross-border data transfer. The U.S. exist two general patterns of privacy protection, industrial self-regulation, and bilateral agreement.[188] The industrial self-regulation through formulates the industrial regulations and

---

184 United States, Executive Office of the President, and John Podesta. *Big data: Seizing opportunities, preserving values. White House, Executive Office of the President*, 2014.
185 United States Federal Trade Commission, "Privacy & Data Security Update" (2017).
186 The Act of United States, *the Clarifying Lawful Overseas Use of Data (CLOUD) Act*, (2018) H.R.4943.
187 Tian, Xu, A Step Forward Made by the US Cloud Act in Cross-Border Jurisdiction, *Journal of Customs and Trade*, 04 (2018), pp.89-101.
188 Zhang, Sheng, "The International Law Regulation Path of Cross-border Data Flows by the United States and China's Countermeasures", *Business and Economic Law Review* (04)2019, pp.79-93.

internal guidelines to protect data privacy when the U.S. corporations transfer data cross-border, specifically, the industrial self-regulation includes formulate the general industrial guidelines and participate in the privacy certification project. In 1998, the U.S. Online Privacy Alliance (OPA) established the *OPA guidelines*, and the OPA guidelines is a recommendatory guideline, it requests that companies within the alliance should formulate a privacy policy that is open to the public to inform network users of the collection and processing of personal data privacy. And two famous American privacy certification agencies, the TRUSTe and BBBOnline based on the OPA guidelines respectively established the privacy protection project and based on the principles of FTC to issue the privacy certification to the corporations who fulfilled the requirements, and the users could through the certification mark to make a choice. The industrial self-regulation through this model to attract enterprises to standardize their data privacy protection mechanisms and conduct privacy certification. Meanwhile, the privacy certification agencies will supervise the companies to continuous compliance review, and penalties are imposed on companies that failed to meet the requirements to ensure the quality of data protection for privacy-certified companies.[189]

Compare with the traditional supervision pattern by the government, the industrial self-regulation is more flexible, and it allowed the corporation to take measures to protect the privacy by themselves, that changed the traditional supervision on the data privacy protection. However, the industrial self-regulation still has several defects, on the one hand, the industrial self-regulation has no legal force, it relies on the corporations' self-discipline, in some conditions, the corporations might sacrifice the personal privacy interest if the individual's privacy has a conflict with the corporations' interest. For example, with the development of big data and cloud computing, personally sensitive information will reflect the consumers' needs and tendencies to the enterprise, and the introduction of privacy policies may affect the analysis of citizens' sensitive information. Therefore, even if an enterprise adopts industrial self-regulation to restrain itself, in view of the non-mandatory binding nature of industrial self-regulation, there may be problems in the actual compliance of the enterprise. On the other hand, since the industrial self-regulation lack the legal binding force, the individuals will face problems on the pursue the remedies when their privacy rights have been infringed. The corporations may not inform users of the data to be collected or transferred in the privacy policy, and in this

[189] Kimery, Kathryn M., and Mary McCord. "Signals of trustworthiness in e-commerce: consumer understanding of third-party assurance seals." *Journal of Electronic Commerce in Organizations (JECO)* 4.4 (2006): 52-74.

case, it is more difficult for the individual to know whether their data privacy rights have been infringed.[190]

The bilateral agreement model on the privacy protection is a complement of the industrial self-regulation, the multinational commerce cannot avoid the massive data cross-border flows, and industrial self-regulation could not provide a legal binding for the requirements of privacy protection. Therefore, the U.S. also through negotiate with other countries or organisations to conclude the bilateral agreement for the data protection on the transborder data flows, like the Safe Harbor agreement, the Privacy Shield agreement. On Jan 12, 2017, the Swiss government announced the Swiss-U.S. Privacy Shied would be an official framework on the data transfer between the Swiss and the United States.[191] The Swiss-U.S. Privacy Shield agreement is similar to the EU-U.S. Privacy Shield agreement that only the corporations which obtained the certification could transfer data between the U.S. and the Swiss, the difference between those two agreements is in the certification process to the corporations. Firstly, the Swiss-U.S. Privacy Shield agreement and the EU-U.S. Privacy Shield agreement together consisted of the Privacy Shield Framework of the United States. The corporations that already listed in the EU-U.S. Privacy Shield and gained the certification, those corporations no need to launch the certificate process again when they are applying the Swiss-U.S. Privacy Shield, and they could directly add their corporations' information in the self-certification. Secondly, U.S. corporations shall take higher responsibility for privacy protection. According to the Swiss-U.S. Privacy Shield agreement, U.S. companies are obliged to provide Swiss data subjects with key information about their personal data, such as whether the data collected involves sensitive data, the purpose of processing the data, and the Conditions of the company's reporting the data to for tripartite transfers, etc. At the same time, companies that need to transfer data cross-border should provide the dispute resolution and retrospect mechanisms applicable to data subjects in the privacy policy of their websites. However, in practice, the U.S. companies might reprocess the personal data transmitted to the U.S., which poses a potential threat to the security of personal privacy information.[192] Therefore, the Swiss-U.S. Privacy Shield request the participants ensuring accountability for data transferred to third parties, that is also the same with the EU-U.S. Privacy Shield, the corporations should ensure the data security when they need to transfer those data to the third party, even when it transfer cross-

[190] Cui, Mengmeng, *Research on Legal Problems of Privacy Protection in Cross-border Data Flows*, East China University of Political Science and Law, 2019.
[191] Swiss and United States, Swiss-US Privacy Shield: better protection for data transferred to the USA.
[192] Cui, Mengmeng, *Research on Legal Problems of Privacy Protection in Cross-border Data Flows*, East China University of Political Science and Law, 2019.

border to the third country. And the participants should take reasonable measures on the remedies and prove that it was compliance with the requirements during the data transfer when they found the third party was failed to provide the adequate level on the protection to the personal data. Otherwise, it will also be responsible for privacy infringement.

3.1.4. The Comments on the Legislation of Transborder Data Flows of Personal Information in the United States

As mentioned on above, the EU and the U.S. on the personal data protection are different, the EU treats the protection on personal information and privacy as the fundamental human right and the consumers' right, the U.S. thought the protection of the personal data and privacy mainly for the protection on the consumers' right.[193] The main objective of the EU's relevant legislation and policies is to focus on the protection of the rights of the data subject and maintain a high level of protection mechanism. The U.S. is encouraging the corporations through commercial use of personal data to make a profit in the business, only under specific conditions, the national authority will get involving and regulate. And most of the States' domestic legislation on personal information protection in the United States also focuses only on consumer rights protection. Therefore, that is not hard to find out the EU's legislation on the protection of the transborder data flows is based on the protection of fundamental human rights, the legislation of the U.S. is leading by the free market.

In practice, the EU arranged the comprehensive mechanism on personal privacy protection, established the independent data supervisory authority and request the data controller and data processor register the information to those supervisory data authorities. And under specific circumstances, the personal data transfer and processing need the pre-authorize as the basic requirements. However, the U.S. has not established any independent legislation on the protection of the personal data cross-border flows, and the relevant regulations are separated in the different industrial acts, the supervision on the personal data protection is more rely on the corporations' self-regulation, like the Safe Harbor framework, the Privacy Shield framework.[194] Besides, the

[193] Aaronson, Susan Ariel, and Patrick Leblond. "Another digital divide: the rise of data realms and its implications for the WTO." *Journal of International Economic Law* 21.2 (2018): 245-272.
[194] Zhang, Sheng, "The International Law Regulation Path of Cross-border Data Flows by the United States and China's Countermeasures", *Business and Economic Law Review* (04)2019, pp.79-93.

U.S. also advocates to arrange a similar mechanism in the "APEC Privacy Framework", the principle of accountability in the APEC Privacy Framework request the personal information controller shall comply with the measures of the framework and take corresponding responsibility. And the personal information controller shall ensure the thirds parties, which receive the personal information from the controller, will fulfil the request of the privacy framework or obtained the unambiguous consent from the individual when personal information controller needs to transfer personal information to the third parties.

The United States values the free flow of data and the economic benefits it brings, therefore, in terms of foreign and external policy, the U.S. only pays attention to market openness and restrictive policies adopted by other countries. The evidence was reflected in the U.S. attitude towards the data protectionism, in 2013, the U.S. International Trade Commission published the "Digital Trade in The U.S. and Global Economies" which defined the data protectionism as the barriers to the digital trade and hindered the data free flows, and other measures on the privacy protection also be defined as the barriers, include the data censorship, the information filtering, the data localization, and privacy protection policy.[195] Besides, this document also specially mentioned the huge difference between the legislation on the privacy protection in other countries caused those countries' lack of interoperability in domestic law, and the costs of the corporations' legal compliance are increasing sharply. Those definitions were made under the situation that the government of the U.S. disregard the privacy protection regulations are based on public interest, national security, and public morality.[196]

3.2. The APEC Legal Framework of Protection of Personal Data Transborder Flows

The Asia-Pacific Economic Cooperation (APEC) is a multilateral economic cooperation organisation designed to encourage the promotion of economic development, cooperation, trade, and investment in the Asia-Pacific region. And the speed and scale of the e-commerce development in the APEC region situate in world-leading position, and the cross-border e-commerce and business of multinational corporations are relying on the

[195] United State International Trade Commission, *Digital Trade in The U.S. and Global Economies*, NO.332-531(2013).
[196] Zhang, Sheng, "The International Law Regulation Path of Cross-border Data Flows by the United States and China's Countermeasures", *Business and Economic Law Review* (04)2019, pp.79-93.

personal data transborder flows, therefore, in 2005, the members of the APEC signed the "*APEC Privacy Framework*" to propose the economic entities respectively through the legislation, policies, and industrial guidelines to implement the APEC Privacy Framework.[197] Although the APEC Privacy Framework has been signed into force by the ministers of members, it has no legal effect on member countries and lacks operability, so it cannot implement effectively.[198] To promote the implementation of the APEC Privacy Framework, in 2007, the APEC Ministerial meeting launched the "*APEC Data Privacy Pathfinder Projec*t" [199] which first-time proposal to establish the general rules on the APEC cross-border privacy protection, then, one of the achievements of the APEC Data Privacy Pathfinder Project was passed the "*Cross Border Privacy Enforcement Arrangement (CPEA)*" [200] in 2009. The CPEA promoted the information sharing and collaboration in enforcement between the privacy protection authorities in the member countries, on the basis of those measures, the APEC formally established the "*Cross-border Privacy Rules System (CBPR)*" in 2013. Therefore, the APEC established a comprehensive cross-border data flow framework which includes the principles of data protection and its enforcement measures. [201]

3.2.1. The Fundamental Principles of the APEC Privacy Framework

The APEC Privacy Framework has four parts, and the first part is the preamble that concludes the objectives of the APEC Privacy Framework, the second part explained the application scope and relevant definitions, the third part is nine principles of the privacy information protection which designed basis on the principals of the the " *OECD Guidelines Governing the Protection of Privacy and the Transborder Flows of Personal Data*"[202], the fourth part is the implementation which from the perspectives of the domestic implementation and international implementation to propose the general rules on the implementation of the APEC Privacy Framework. Although the APEC Privacy Framework did not set up a specialize chapter for the cross-border

---

[197] Asia-Pacific Economic Cooperation, "APEC Privacy Framework," *Asia Pacific Economic Cooperation Secretariat* 81 (2005).
[198] Greenleaf, Graham. "Five years of the APEC Privacy Framework: Failure or promise?." *Computer Law & Security Review* 25.1 (2009): 28-43.
[199] Asia-Pacific Economic Cooperation, "*APEC Data Privacy Pathfinder Projects Implementation Work Plan*", 2009/SOM1/ECSG/SEM/027.
[200] Asia-Pacific Economic Cooperation, "*The APEC Cross-border Privacy Enforcement Arrangement (CPEA)*", 2010/SOM1/ECSG/DPS/013, available at: http://cbprs.org/wp-content/uploads/2019/11/1.-Cross-Border-Privacy-Enforcement-Arrangement-updated-17-09-2019.pdf .
[201] Yong-qin, Gong, and Wang Jian. "Comparison of Cross-border Privacy Rules of APEC and EU." *Asia-pacific Economic Review* 5 (2015): 4.
[202] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), OECD, available at: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm .

data flow, the relevant rules of personal data transborder flows still reflected in the part of information privacy principles and implementation.

The most important principles of the APEC Privacy Framework we already mentioned above, the principle of accountability.[203] According to the principle of accountability, the personal information controller shall take two kinds of responsibility, and firstly, the personal information controller shall complying with the requirements of the APEC Privacy Framework. Secondly, they still should take responsibility for the activities of the third party and ensure the third party obeying all the principles of the APEC Privacy Framework. Besides, the principle of accountability also exists the flexibility of its implementation, it allowed the personal information controller to maintain the legal basis of the personal information transfer by gained the unambiguous consent of the individual when the relation between the personal information controller and the third party does not exist anymore, and the personal information controller is difficult to ensure the third party to provide the adequate protection on the personal information.

In the implementation of the APEC Privacy Framework, it regulated if a member economy already through the legislation or the supervisorial policies to implement the APEC Privacy Framework or provide the adequate measures on personal information protection and personal information controller could keep to complying the requirements of the APEC Privacy Framework and other relevant domestic laws, the other member economies cannot restrict the personal data cross-border flows to this kind of member economy. Therefore, the APEC put the accountability principle as the core rules of the cross-border data flow and request the personal information controller take responsibility for the personal information transfer to protect personal privacy.[204]

[203] Asia-Pacific Economic Cooperation, "APEC Privacy Framework," *Asia Pacific Economic Cooperation Secretariat* 81 (2005), principle of accountability.
[204] Yong-qin, Gong, and Wang Jian. “Comparison of Cross-border Privacy Rules of APEC and EU.” *Asia-pacific Economic Review* 5 (2015): 4.

3.2.2. The APEC General Model of the Protection of Personal Information Cross Border Transfer

As the core principle of the APEC Privacy Protection, the accountability principle not only reflect in the APEC Privacy Framework but also implement in the cross-border privacy protection framework, the Cross-border Privacy Rules System (CBPR). The CBPR is aiming to find a solution to the personal information free flows between the member economies and strive for non-barriers personal information flows basis on adequate protection. Meanwhile, the CPBR system is a voluntary, accountability-based system that facilitates privacy-respecting data flows among APEC economies.[205] To achieve the personal information free flows between the APEC economies, the CBPR system from perspectives of the privacy enforcement authority, the accountability agent and the corporations to design the framework of the system to ensure the participants' privacy protection could reach the standards of the CBPR.[206]

a) The privacy enforcement authority

The precondition of the participating in the CBPR system is the located economies of the corporation at least have a privacy enforcement authority joined the APEC Cross Border Privacy Enforcement Arrangement (CPEA). Normally, the infringement in the personal information cross border transfer always happened in a foreign country, and the domestic privacy protection authority was bound by domestic law that cannot make a penalty to the foreign infringer. Therefore, that needs the privacy enforcement authority of infringer' country takes action. And the CPEA provides the multilateral and interoperable mechanism on privacy enforcement for the privacy enforcement authority in the APEC economies, and the privacy enforcement authorities could provide cooperation arrangement for cross-border privacy enforcement via the CPEA voluntarily, like share the information and proposal the specific enforcement plan.[207] And the CPEA defined the privacy enforcement authority is any public body that responsible for the enforcement of the privacy laws, and that has powers to conduct investigations or pursue enforcement proceedings.[208] Any privacy enforcement

---

[205] Asia-Pacific Economic Cooperation, "*About CBPR*", available at: http://cbprs.org/about-cbprs/ .
[206] Asia-Pacific Economic Cooperation, "*APEC Cross-Border Privacy Rules System, Policies, Rules and Guidelines (Updated as of November 2019)*", available at: http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf .
[207] Asia-Pacific Economic Cooperation, "*The APEC Cross-border Privacy Enforcement Arrangement (CPEA)*", 2010/SOM1/ECSG/DPS/013, available at: http://cbprs.org/wp-content/uploads/2019/11/1.-Cross-Border-Privacy-Enforcement-Arrangement-updated-17-09-2019.pdf .
[208] Asia-Pacific Economic Cooperation, "*APEC Cross-Border Privacy Rules System, Policies, Rules and Guidelines (Updated as of November 2019)*", p. 10, available at: http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-

authorities of the APEC economies could join the CPEA but need the economies to propose the application to the APEC, then, when economies want to join the CBPR, the Joint Oversight Panel (JOP) will take the investigation to the economies' privacy enforcement authorities to ensure they have the power to enforce the principles of the APEC privacy framework.

b) The accountability agent

When economies apply to join the CBPR, the economies also need at least have an accountability agent, which recognized by APEC, to responsible for the operation of the CBPR system. The accountability agent should be supervised by the APEC, and it has the power to issue the certification to the business entities, and it could be the public sector or private sector. The accountability agent is responsible for certifying the personal data protection level of the corporation that apply to join the CBPR system and ensure those corporations to satisfy the requirements of the CBPR and the APEC Privacy Framework and provide the disputes solution mechanism for the individuals.[209] The accountability agent is the key to the CBPR system. Hence, the APEC take strict criteria on the recognition of the accountability agent. After receipt of a request for recognition pursuant of the accountability agent, the JOP will initial the investigation and then issue the recommendation to the APEC economies, if the APEC economies did not object the recognition, the request would be approved by the Electronic Commerce Steering Group (ECSG).[210] Besides, the APEC recognition of the accountability agent will be limited in one year from the date of recognition, and thee accountability agent should re-apply one month prior to the deadline.[211] The accountability agent is an innovation of the CBPRsay y,stem which basis on the accountability principle, and it enhanced the enforcement of the CBPR and APEC Privacy Framework and played an important role in the CBPR system.

c) Thparticipant'sts corporations

After the accountability agent obtained the recognition from the APEC, the domestic corporations could request the certification of the privacy protection to the local accountability agent to achieve the free flows of

---

Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf .

209 Asia-Pacific Economic Cooperation, "Cross Border Privacy Rules and Privacy Recognition for Joint Oversight Panel", 19 Feb 2013, as amended 18 June 2013.

210 Asia-Pacific Economic Cooperation, "*APEC Cross-Border Privacy Rules System, Policies, Rules and Guidelines (Updated as of November 2019)*", para. 33, available at: http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf .

211 Asia-Pacific Economic Cooperation, "*APEC Cross-Border Privacy Rules System, Policies, Rules and Guidelines (Updated as of November 2019)*", para. 36.

the personal data under the CBPR system. And the foundation of the CBPR system is the corporations' self-certificate mechanism, and the applicant shall intake the questionnaire to self-censor is their privacy protection policies comply with the requirements of the APEC Privacy Framework or not.[212] Then, the accountability agent will examine the privacy protection level of the applicants, if the situations could fulfil the requirements of the CBPR, the accountability agent will issue the certification and approve the applicants participate in the CBPR system.

3.2.3. The Comments on the APEC Legal Framework of Protection of Personal Data Transborder Flows

The most peculiarity characters of the APEC legal framework of protection of personal data transborder flows is the accountability principle as the core of the whole system, it requests the CBPR system participants take the responsibility of the personal information cross border transfer, put it in another word, the APEC is focused on the protect the personal privacy implementation, not the destination of the data flows, its organisationally-based not the geographically-based, and that is also the obvious difference between the EU model and the APEC model.[213] Undoubtedly, the APEC model also exists several defects in the practice.

Firstly, the APEC exclude the responsibility of the accountability agent. The APEC Privacy Framework defined the personal information controller is "*a person or organization who controls the collection, holding, processing or use of personal information*".[214] Obviously, the accountability agent has been excluded of the responsible bodies, consequently, if the accountability agent violates the corporations' willing and the principles of the APEC Privacy Framework, the accountability agent no need to take the responsibility and the corporations also could via obtained the personal information subjects' consent to defence. Theoretically, the APEC Privacy Framework provides the possibility that the accountability agent could avoid the responsibility, that is also made the personal information subjects are difficult to pursue the remedies when they have been infringed.[215]

---

[212] Asia-Pacific Economic Cooperation, "*CBPR Intake Questionnaire*", available at: https://cbprs.blob.core.windows.net/files/Cross%20Border%20Privacy%20Rules%20Intake%20Questionnaire.pdf .
[213] Yong-qin, Gong, and Wang Jian. "Comparison of Cross-border Privacy Rules of APEC and EU." *Asia-pacific Economic Review* 5 (2015): 4.
[214] Asia-Pacific Economic Cooperation, "APEC Privacy Framework," *Asia Pacific Economic Cooperation Secretariat* 81 (2005), Article 10.
[215] Israel, Barbara A., et al. "Critical issues in developing and following CBPR principles." *Community-based participatory research for health: Advancing social and health equity*(2017): 31-46.

Secondly, the CBPR system lacks supervision on the personal information cross border flows. The accountability principle emphasizes the corporations' self-regulation. Actually, that is heavy burdens for the corporations. The accountability principle requests the corporations to ensure every transfer of the personal information should comply with the requirements of the CBPR, in practice, it not only adds the compliance cost of the corporation but also might impact the corporations' measures on the privacy protection because that is difficult to continually supervise the personal information transfer, especially for the SMEs. Under this kind of situation, the corporations might take down the level of privacy protection to control costs, undoubtedly, that will bring disadvantages influence to the individual's rights and multinational commerce. Moreover, at present, the CBPR participants and corporations are limited, the operation of the CBPR system also not consummate that did not have a widespread influence in the APEC region.[216]

Compared with the legislation of the EU on the protection of transborder data flows, the EU model was based on the adequate level of protection and established the consistent standards on the data cross border flows, it beneficial to the stable order on the personal privacy protection and provide individuals with reasonable expectations. However, the high criteria on the transborder data flow also restrict the free flows of the data and hinder the development of multinational commerce. The APEC model is based on the CBPR system which almost relies on the accountability principle, and the accountability principle almost rely on the corporations' self-regulation, the privacy enforcement authority will only intervene when the infringement already happened. Undoubtedly, it will promote the personal information cross border flows, but it also put the heavy burdens on the corporations' shoulders, and that might cause the disadvantages influence both to the economy and individual's privacy. On the enforcement of the regulation, the EU model is stronger than the APEC model, and on the fundamental principle, the EU chooses the geographically-based adequate level of protection, the APEC chooses the organisationally-based accountability principle. It is difficult and almost impossible to define which system is perfect for both economy and personal privacy protection, but in my opinion, the perfect situation for the EU is to absorb the advantages of the APEC model and complete and improve the regulations on the transborder data flow, trying to find an ideal balance between the free flow of the data and the protection of the personal privacy.

---

[216] Israel, Barbara A., et al. "Critical issues in developing and following CBPR principles." *Community-based participatory research for health: Advancing social and health equity*(2017): 31-46.

3.3. The Legal Framework of Protection of Personal Data Transborder Flows in China

According to the "*The 44th China Statistical Report on Internet Development*", China has 854 million internet user, and internet penetration rate reached 61.2% until June 2019, and the scale of the digital economy in 2018 reached 31.3 trillion RMB, accounting for 34.8% of GDP.[217] And the "*2018-2019 China Cross-border E-commerce Market Research Report*" indicated the scale of Cross-Border E-Commerce industry transactions in China reached 9.1 trillion RMB in 2018, and the scale of users exceeded 100 million.[218] Undoubtedly, China already standing in the leading position of the international digital economy and with the "Belt and Road" policy, the cross-border e-commerce will be developing sharply. Therefore, the regulations on the cross-border data flow should be following the development of the digital economy to provide a favourable business environment for economic development and individuals' right protection.

3.3.1. The Legislation on Personal Data Transborder Flows in China

Until present, China did not publish a consistently personal data protection law, the relevant rules which regulate the personal data transborder flows are separated in different laws, regulations, and directives, hence, that caused the difficulties in the enforcement. The first legal document of the personal information cross border flow is to regulate the financial field in 2011, the "*Notice by the People's Bank of China Regarding the Effective Protection of Personal Financial Information by Banking Institutions*", that request the banking financial institutions stored, processed, and analysed personal financial information inside China cannot transfer those information cross border to other countries or regions.[219] Then, in 2013, the Art 24 of the "*Regulation on the Administration of Credit Investigation Industry*" reaffirm this rule that credit investigation

---

[217] China Internet Network Information Center, "*The 44th China Statistical Report on Internet Development*", Aug 2019.
[218] iiMedia Research, "*2018-2019 China Cross-border E-commerce Market Research Report*", 22 Mar 2019, available at: https://www.iimedia.cn/c400/63893.html .
[219] People's Bank of China, "*Notice by the People's Bank of China Regarding the Effective Protection of Personal Financial Information by Banking Institutions*", No.17 (2011) of the People's Bank of China, 21 Jan 2011, para 6.

institutions shall set up the database and arrange store, and process the information inside of China.[220] Obviously, the early legislation trends of personal data cross border flow in China supported the data localization, especially for sensitive personal information. Besides, these contents two articles real ambiguous and the statutory exemptions also not detailed, only regulate the personal information cross border in the financial field and did not clarify the accountability and the remedies.[221]

The first comprehensive industrial guideline of the personal information protection was published in November 2012, the "*Information Security Technology - Guidelines for the Protection of Personal Information in Public and Commercial Service Information Systems*".[222] The Article 5.4.5 of the guideline regulated the personal information cross border flow will not be restricted if the personal information exporter obtained the consent from the personal information subject, or the competent department, or has other explicit legal bases.[223] Besides, for the consent of the personal information subject, the guideline distinguished the conceptions of the acquiescence consent and explicit consent. However, the guideline still did not clarify the detailed situation of the consent of the competent department and other explicit legal bases. Meanwhile, this guideline is a departmental regulatory document that without the legally binding, only provide the basic directions to the corporations and rely on themselves to enforce the guideline.[224]

Then, on 1 June 2017, the "Cybersecurity Law of China" has been published by the Standing Committee of the National People's Congress of China.[225] The Cybersecurity Law not only regulate the network operation security but also established the network information security system, which includes personal information protection. According to the Article 37 of the Cybersecurity Law, if the critical information infrastructure operators indeed necessary of the business requirements to transfer personal data cross border, they shall

---

[220] State Council of China, "*Regulation on the Administration of Credit Investigation Industry*", No.631 Order of the State Council, 21 Jan 2013.
[221] Zhifang, Ji, "Research on the Legal Regulation of the Cross-border Flow of Personal Financial Information", Huabei Finance, 08 (2015), pp43-46.
[222] Inspection and Quarantine and the Standardization Administration of China, "*Information Security Technology - Guidelines for the Protection of Personal Information in Public and Commercial Service Information Systems*", GB/Z 28828-2012, 5 Nov 2012.
[223] Inspection and Quarantine and the Standardization Administration of China, "*Information Security Technology - Guidelines for the Protection of Personal Information in Public and Commercial Service Information Systems*", GB/Z 28828-2012, 5 Nov 2012, Article 5.4.5.
[224] Hu, Wei, "Value Orientation and China's Choice on Transborder Data Flow", *Journal of Social Sciences*, 04 (2018), pp. 95-102.
[225] Standing Committee of the National People's Congress of China, "*Cybersecurity Law of China*", No.53 Order of the President of the People's Republic of China, 1 June 2017.

accordance with relevant measures to pass the security assessment.[226] That shows the Chinese attitude to the data transborder flows are different from Russia that prohibits any forms of data transfer cross border, and also different from the U.S. that no pre-condition for the data cross border flows. The Cybersecurity Law is a step forward of the legislative framework on the transborder data flow. However, several definitions still are ambiguous, like the scope of the information data, the detailed processes of the security assessment.[227] Therefore, the Cyberspace Administration of China (CAC) released the "*Security Assessment for Personal Information and Important Data to Be Transmitted Abroad (Draft for comments)*" to support the enforcement of the Cybersecurity Law on 11 April 2017,[228] it clarified the condition, criteria, and period of the security assessment of the data transfer cross border and expanded the scope of the subjects of the security assessment, from the "critical information infrastructure operators" to the "network operator".[229] Then, two years after, on 13 June 2019, the CAC released the revised version, the "*Measures on Security Assessment of the Cross-border Transfer of Personal Information (Revised draft)*", the main changes include it the security assessment period from every year change to them every two years or whenever the purpose, types or extraterritorial retention period of the cross-border transfer of personal information has changed and amplified the requirements of the contracts between the network operator and the personal information receiver. On 6 March 2020, the Standardization Administration of China (SAC) released the "*GB/T 35273-2020 Information Security Technology – Personal Information Security Specification (2020 PISS)*" to replace the "*GB/T 35273-2017 Information Security Technology – Personal Information Security Specification*".[230] The structures and definitions of the Personal Information Security Specification are really similar to the GDPR. Thus somebodies call it the "Chinese GDPR".[231] Although the Personal Information Security Specification is a recommended national standard for the industry, it still is a basic standard for the personal information protection, and the specific regulation or law has not come out yet, it will be an important reference for the further legislation on the personal information protection. Therefore, the domestic legal framework of the

---

[226] Standing Committee of the National People's Congress of China, "*Cybersecurity Law of China*", No.53 Order of the President of the People's Republic of China, 1 June 2017, Article 37.
[227] Hu, Wei, "Value Orientation and China's Choice on Transborder Data Flow", *Journal of Social Sciences*, 04 (2018), pp. 95-102.
[228] Cyberspace Administration of China, "*Security Assessment for Personal Information and Important Data to Be Transmitted Abroad (Draft for comments)*", 11 Apr 2017.
[229] Liu, Jinrui, "Comments and Proposals regarding the Provision on the Security Assessment for Personal Information and Important Data to Be Transmitted Abroad (Draft)", *Information Security and Communications Privacy*, 06 (2017), pp. 72-78.
[230] Standardization Administration of China, "*Information Security Technology – Personal Information Security Specification*", GB/T 35273-2020, 6 Mar 2020.
[231] Hong, Yanqing, and Ge, Xin, "Interpretation of National Standard 'Information Security Technology – Personal Information Security Specification'", *Secrecy Science and Technology*, 08 (2019), pp.24-28.

personal data cross-border flow in China already established and will keep amplifying the personal information protection system.

3.3.2. The General Model of the Personal Information Cross-border Flow in China

According to the "*Measures on Security Assessment of the Cross-border Transfer of Personal Information (Revised draft)*" and the "*GB/T 35273-2020 Information Security Technology – Personal Information Security Specification (2020 PISS)*", at present, the general models of the cross-border transfer of personal information are personal information subject's consent and the security assessment. In GDPR, the data subject's consent was the statutory exceptions of the principle of the adequate level of protection and the Chinese security assessment mechanism also seems like the BCRs of the GDPR.[232]

3.3.2.1. The Consent of the Personal Information Subject

a) The requirements of the personal information collection

Article 5 of the 2020 Personal Information Security Specification listed the requirements of the personal information collection, including the legitimacy of the collection, the minimum necessities, the consent of personal information subject, and the exception of the consent. The Article 5.4 stipulated the personal information controller shall inform the purposes, forms, and scope of the personal information collected to the personal information subject and the when collecting the sensitive personal information, the personal information subject has the self-selection right for automatic collection, besides the personal information controller has the liability to inform the results might bring by personal information subject's decision. For example, if the personal information controller objects the collecting the sensitive personal information for the extended business or functions, the personal information controller cannot refuse to provide the basic business on the ground of the personal information subject's objection.

b) The exceptions of the consent of the personal information subject

---

[232] Liu, Jinrui, "Comments and Proposals regarding the Provision on the Security Assessment for Personal Information and Important Data to Be Transmitted Abroad (Draft)", *Information Security and Communications Privacy*, 06 (2017), pp. 72-78.

Article 5.6 of the 2020 Personal Information Security Specification illustrated the 11 exceptions that the collection of personal information could without the consent of the personal information subject, those exceptions could be summarized into the following types: 1) interrelated with the national security and public interest; 2) interrelated with the criminal investigation, prosecute and other judicial procedures; 3) protect the personal information subject's interest or third-party's interest; 4) public disclosure by personal information subject or collected from other legitimate measures; 5) necessary to maintain the security and stability of the products or services provided; 6) for legitimate news reporting or academic research

c) The withdraw of the consent

Article 8.4 of the 2020 Personal Information Security Specification stipulated the personal information subject has the right to withdraw the consent, and then the personal information controller shall provide the scheme of the consent's withdraw to the personal information subject, besides, the personal information subject also could withdraw the consent to object receiving the commercial advertisement which based on their personal information. One thing that should be mentioned that withdraws the consent will not affect the prior processes on personal information.

3.3.2.2. Security assessment of the cross-border transfer of personal information

a) The forms of the security assessment

The forms of the security assessment include the network operator's self-assessment and the assessment from the cybersecurity administration. The self-assessment of the network operator only could be launched when the purposes and the scope of the personal information transfer cross-border have fundamental changes or happened the security incidents or the request of the industrial authorities or supervisory authorities. And the network operator shall designate an assessment group which includes the consisting of legal and technical experts, then assessment group will review and evaluate the network operator's personal information protection mechanism, and according to the purposes of the personal information transfer and the security risks to issue a report, the network operator shall submit the reports to the relevant authority for the review and filing. The cybersecurity administration and the industrial authorities could launch the security assessment when the personal information transfer linked with the public interest or name security, then the cybersecurity

administration and the industrial authorities will form an assessment working party to confirm the scope of the assessment and formulate the detailed assessment plans, then the specialised committee will review the report of the assessment working party and issue the recommendations to the cybersecurity administration and the industrial authorities.

b) The contents of the security assessment

The contents of the security assessment mainly about the assessment of the security risks and the assessment of the purposes of the personal information transfer, like the legitimacy and necessity of the transfer, for example, whether the purposes of transfer is in compliance with the relevant laws and regulations, whether the consent of the personal information subject has been obtained, whether it is necessary to perform contractual obligations or business. In the assessment of security risks, the attributes of personal information and the possibility and scope of security incidents during transfer cross-border are mainly considered, and the assessment of the personal information's attributes will be based on the elements like amount, scope, sensitivity, and technical processing status. In the assessment of the security incidents' possibility and impact will mainly base on the technical and administrative ability of the personal information controller, the network security level of the personal information received and the recipient's measures on the protecting the personal information cross-border transfer, the laws and policies and relevant legal environment of the recipient's country or region.

3.3.3. The Comments on the Legal Framework of Personal Information Transfer Cross-border in China

Apparently, the personal information transfer cross-border in China are based on the "consent of the personal information subject" and the "security assessment" which also exist several defects. For the "consent of the personal information subject", the "*Measures on Security Assessment of the Cross-border Transfer of Personal Information (Revised draft)*" classifieds the personal information include the sensitive personal information and non-sensitive personal information, the personal information controller collecting the non-sensitive personal information only needs to obtain the acquiescence consent not the explicit consent, hence, that will cause the personal information to be collected, and the personal information subject was not noticed. Besides,

when the personal information controller indirectly collects personal information, they need to ensure the legitimacy of the collection of personal information. However, most of the data transactions are operating online, and it is difficult to trace to the source and to review the authenticity, undoubtedly, the burdens on the personal information controller are heavily again.[233]

For the "security assessment", firstly, the definitions of the security assessment launch conditions are ambiguous, like express of the "fundamental changes" and "major security incident", according to the rules of the self-assessment, did not have an explicit criterion and interpretation, the personal information controller needs to judge by themselves, that will not only cause inconsistent enforcement but also might infringe the personal information subject's rights. For the "assessment from the competent department", the cybersecurity department of the industrial administration should assess the elements for the personal information transfer cross-border like, data which related with the critical information infrastructure, the security risk and defects, and the specific security response solution of the personal information controller. Actually, some contents of these two assessment measures are similar that might cause conflicts and problems in implementation.[234] And some requirements of the personal information controller's self-assessment are difficult, and even almost impossible for SMEs, for example, the self-assessment request to assess the "laws, regulations, and relevant legal environment of the personal information receiver's country or region", these kinds of assessment unquestionable required to hire the experts and will cost numerous budget and manpower, put it in another word, it could be treated as a restriction for the personal information transfer cross-border.

The "*Outline of the 13th Five-Year Plan for the National Informatization*" declared the objective that established the security supervisory system of the cross-border data flow[235], the present legislation of China are focus on the protection of cyberspace sovereignty and national security, the protection of the personal information transfer cross-border have not got sufficient emphasis, and that might introduce the disadvantageous impact to the development of the cross-border commerce.[236] Moreover, for the perspective

---

233 Liu, Jinrui, "Comments and Proposals regarding the Provision on the Security Assessment for Personal Information and Important Data to Be Transmitted Abroad (Draft)", *Information Security and Communications Privacy*, 06 (2017), pp. 72-78.
234 Hong, Yanqing, and Ge, Xin, "Interpretation of National Standard 'Information Security Technology – Personal Information Security Specification'", *Secrecy Science and Technology*, 08 (2019), pp.24-28.
235 State Council of China, "*Outline of the 13th Five-Year Plan for the National Informatization*", No.73 (2016) Order of the State Council, 15 Dec 2016.
236 Qi, Aiming, "On the Improvement of the Comprehensive Legal Protection of Data Security in the Big Data Era——From the View of Cyber Security Law", *Journal of Northeast Normal University (Philosophy and Social Sciences)*, 04 (2017), pp. 108-114.

of the legislation of the laws and regulations, the specific legal instruments on personal information protection have not come out yet, the relations between the protection of the personal information subject's right, the cyberspace sovereignty, and the development of the economy still are ambiguous. Obviously, China needs to publish consists, comprehensive, and unambiguous laws to resolve those problems.

Conclusion

1. The Impact of Personal Data Definition and Consent Clause

The orientation of the EU's personal data transfer regulations is protecting the fundamental rights of individuals, and it embodies the protecting personal dignity and honour. Therefore, the definition of personal data will directly reflect the scope of the individuals' rights and data transfer regulations. In the big-data era, with the development of the technologies and social consciousness, the definition of personal data has further expanded, like the physiological and genetic factors also will be treated as personal data.[237] More specifically, the present personal data has the following characteristics: firstly, the uses of personal data are comprehensive in the big-data era, which differs from the traditional uses. After anonymizing the personal data as the original data, it is still valuable for reprocessing of the digital services and applications. Meanwhile, the individuals' decision will be limited by their technological skills and inadequate rational analysis, at least compared to big data technology, individuals often cannot make accurate and timely predictions of data usage decisions based on ICTs, but the re-analysis and application of data by big-data could maximize the value of data. Put it in another, the decisions made by computers are more rational, reasonable, and profitable then humans' choice.[238] Secondly, the personal data subjects' rights are not the absolute right anymore. In the traditional theory, the personal privacy right is regarded as the right of a natural person to control his or her personal information, private activities and private domains that are not related to the public interest, it emphasizes the strict boundaries of physical space. However, with the development of the ICTs, the data is not just the information stored in the physical container and could be controlled by individuals, like paper documents, floppy disk, and CD, at present, at present, the data normally stored in the serves and connected with the internet, hence, the personal data subjects are hard to obtain the full control of their data. Moreover, the data are naturally shareable, and it also includes the personal data generated on the network. Or we could conclude the data on the internet was made for the sharing and flows.[239] Thirdly, the big-data does not require the absolute accuracy of the data.

---

[237] Regulation (EU) 2016/679, *GDPR*, *OJ* L 119, 4 May 2016, Article 4 para. 1, "'*personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person,*".

[238] Wu, Weiguang, "Critique of Personal Data Protection Theory under Big Data Technology", *Political Science and Law*, 07 (2016), pp. 116-132.

[239] Wu, Weiguang, "Critique of Personal Data Protection Theory under Big Data Technology", *Political Science and Law*, 07

The traditional approach of the statistics was boundary by the technology, the information collected is relatively small and often through the sampling surveys, it is necessary to ensure that the recorded information is accurate to keep the results in the scope of a normal error-tolerance rate. However, the big-data are based on the extremely large amounts of data to conduct the analysis, while abandoning the accuracy of mass data, it has obtained more powerful conclusions based on quantity and algorithms. The simple algorithms for big data are more effective than complex algorithms for small data, and that whole samples based on confounding can achieve more accurate results than sampling surveys,[240] it is neither realistic nor advantageous to pursue the accuracy of the data in nowadays.

Therefore, the undying logics of the legal structures of the personal data subjects' rights are based on the traditional society's information processing approaches, not the new ICTs. Obviously, it will cause conflicting practices, especially might drag the personal data subject into the trouble when they click the consent option of the privacy policy. The consent clause not only is treated the true expression of the informational self-determination but also is the prior legal basis of the personal data processing.[241] The consent clause of the GDPR stipulated the personal data subject has the rights to consent the transfer of their data cross-border to the third-countries or region which cannot provide the adequate level of protection[242], although it also required to obtain the explicit consent of personal data subject and the strictly formal requirements[243], and even stipulated the personal data subject has the right to withdraw the consent[244], but it still cannot ensure every user will carefully read and totally understand the privacy policy of the data controller or processor. In practice, when user wants to get the online services or applications, they always need to read dozens of pages of the privacy policies, general clauses, and conditions, the user only has two choices for those paper works, accept or not. And the users cannot access the services or applications if they refused those provisions. Meanwhile, those provisions also cannot negotiate and be revised, and it is a standard form contract. Actually, that is not uncommon, almost all of the data controller and data processor obtained the personal data subjects' consent through this approach, and the users already used to this mechanism. The consent clauses of the GDPR might

(2016), pp. 116-132.
240 Mayer-Schönberger, Viktor, and Kenneth Cukier. *Big Data: A Revolution That Will Transform How We Live, Work and Think*. London: John Murray, 2013. Print, p. 88.
241 Regulation (EU) 2016/679, *GDPR*, *OJ* L 119, 4 May 2016, Article 6 para. 1(a).
242 Regulation (EU) 2016/679, *GDPR*, *OJ* L 119, 4 May 2016, Article 49 para. 1(a).
243 Article 29 Data Protection Working Party, Article 29 Working Party Guidelines on consent under Regulation 2016/679, WP259 rev.01, 28 Nov 2017.
244 Regulation (EU) 2016/679, *GDPR*, *OJ* L 119, 4 May 2016, Article 7 para 3.

bring a kind of illusions to the data subject that they are re-controlling their data, but in fact, the liability already been transfer to themselves by their consents. Therefore, in practice, the consent clause maybe cannot provide adequate protection to personal data even could be used by the data controller or data processor to escape responsibility.

Under this kind of circumstances, the EU could improve the consent clauses by following suggestions, firstly, improve the classification and hierarchy of personal data, although the Article 9 of the GDPR list the several special categories of personal data and its processing requirements, it still has not set up the hierarchical system for personal information. An unambiguous personal information hierarchical system that has several different layers and levels for the various personal information is not only helpful for the delicate management for the information, it distinguishes the processing requirements of different personal information, but also could relieve the companies' compliance burden. Moreover, the hierarchical system also could classify the data controller and data processor based on their core business, the scale of data they control or processing, the purposes of data processing, etc. And according to the hierarchy to stipulate varying degrees, responsibilities for data controller and data processor. Secondly, limit the general authorization terms in the privacy policies of the data controller and data processor, and clarify the scope of authorization. The data controller and data processor shall make a reasonable effort to ensure the data subjects will take notice of the authorization contained in the privacy policies, not just listed in lengthy and tiny characters. Besides, if the data subject does not agree to the authorization of additional functions, they should not affect their use of core functions. And the content of the privacy policies should add the evaluation of the data risks, the data subject not only should be informed the liability when they accept the privacy policies but also has the right to know what kinds of risk their data will face.

2. The Data Localization, the Data Sovereignty, and the Long-Arm Jurisdiction

The GDPR was followed the basic mechanism of the transborder data flow in the Data Protection Directive, the adequate decision as to the core measure and supplement with other measures, like the statutory exceptions, the consent clauses, the SCC, the BCRs, the Privacy Shield framework, etc. Through the analysis all those

measures on above, we still could easily find the standards for the personal data transfer still keeping in a high level, undoubtedly, it will influence the data free flow, especially after the *Schrems* case. The *Schrems* case announced the personal data transfer cross-border under the Safe Harbor framework was violated the EU laws and infringed the personal data subject's rights, besides, the ECJ has also hinted that stored the personal data in the servers within EU boundaries are more suitable fulfil the requirements of the EU laws.[245] Therefore, the data localization suddenly provoked interest in the digital business circle, and numbers of U.S. corporations declared they have the servers which stored the data in EU borders or announced they would launch the plan to store data in the EU.[246]

Although the data localization does not mean the definite prohibition on the data transfer cross-border, the requirements for the corporations to storage the data in EU borders still is not a small burden, according to the research on the costs of the data localization, the forced data localization policy will increase the company's cost by 30% to 60% on the data local storage.[247] And for the EU Internet companies, there also should spend the same costs on the data storage in other countries, some Internet companies might close the abroad business if the profit could not support the abroad marketing, and that will influence the competitiveness of EU digital economy. Almost all of the data localization policies are announced it is aiming for personal privacy protection and national security, but the question is whether the data stored in physical boundaries could really provide a good environment for the data protection, and I doubt it. Although the physical servers are located in physical lands and could be controlled by owners, the servers functioning cannot without the support of the network, and once it connects with the Internet, theoretically, the influence of the physical boundaries will vanish immediately. And once the data transfer has happened, technically, the traces are hard to be hindered and deleted.[248] And with cooperation between national intelligence agencies, like the U.S. National Security Agency (NSA) and the UK signals intelligence service Government Communication Headquarters (GCHQ) is particularly close, the information sharing also conducted between those authorities in many countries, the data localization seems could not ensure all the receptor provide the adequate protection for those data.[249]

---

[245] Joined Cases C-203/15 and C-698/15, Tele2 Sverige & Secretary of State for the Home Department, ECL:EU:C:2016:970, 21 December 2016, para.114, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CA0203 .
[246] Ahmed, Mured, and Richard Waters. "Microsoft unveils German data plan to tackle US internet spying" *Financial Times* (2015).
[247] O'Connor, Brendan. "Quantifying the Cost of Forced Localization." *Leviathan Security Group, June* (2015).
[248] Tian, Xu. "Rising and reflection of data localization legislation", *Journal of Dalian Maritime University (Social Science Edition)*, 01 (2020), pp.32-40.
[249] Kuner, Christopher. "Reality and illusion in EU data transfer regulation post Schrems." *German Law Journal* 18.4 (2017): 881-918.

Actually, the underlying purpose of the data localization is to maintain the data sovereignty and hold the whole jurisdiction on the cases linked with data. Some views treated the data sovereignty is the extend of the national sovereignty in the cyberspace and digital world[250], in fact, national sovereignty, as the fundamental principle of international law, which also based on the territorial sovereign. However, the theory which could support territorial sovereignty also could extend to cyberspace are not exist. Therefore, I think the most important political considerations on the data localization is to hold the jurisdiction of the cross-border data flow. The international law has not yet developed customary law of national jurisdiction for cyberspace. Hence, territorialism has become a reliable basis for national jurisdiction over cyberspace. Although cyberspace is virtual, the servers where the data is stored is physically exist, and the territorial jurisdiction still could be applied in the personal data transfer cross-border.[251] Moreover, the GDPR also stipulated the long-arm jurisdiction on the personal data protection, and Article 3 extended the territorial scope of the GDPR that could regardless of the physical boundaries to prosecute foreign companies, in practice, this means any companies, that supply goods or services to the EU, should comply with the GDPR, regardless of whether the company is located. Therefore, through the long-arm jurisdiction, the EU could force the multinational corporations, which aspire the European market, to following the requirements of the GDPR and conduct their business model to fit the EU model. Combining with the implementation of the data localization and long-arm jurisdiction, it like the two shields for both the individual's rights and the blueprint of the EU digital and internet industry. All those arrangements definitely reflect the EU still trying to take the dominant position in the global digital economy, although the EU digital and internet industry are weak compare with the U.S. and China.

3. The International Cooperation and Multilateral Protection Mechanism

Through analysis of the worldwide legislation on the personal data protection of transborder data flow, essentially, the common dilemma is how to keep the perfect balance between the protection of the human

[250] Qi, Aiming, & Pan, Jia, "Right to Data, Data Sovereignty and the Basic Principle of Big Data Protection", *Journal of Soochow University (Philosophy & Social Science Edition)*, 36 (2015), pp.64-70.
[251] Tian, Xu. "Rising and reflection of data localization legislation", *Journal of Dalian Maritime University (Social Science Edition)*, 01 (2020), pp.32-40.

rights and the data free flow. The transborder data flow is not only a domestic problem, but it also connects with the international dimension, which needs to coordinate the domestic and external policies, however, the objectives and measures of each political entities are naturally different and exists the conflicts and competitions. And with the natural characters of the network and internet industry, that the data only valuable when it flows and be used. It is almost impossible for a single country or region, or several countries, to effectively implement and enforce domestic personal data protection systems. The transborder data flow makes the implementation of personal data protection measures require the joint efforts and active participation of the international community and various countries. The regulations and policies of the transborder data flow should not only take into force in EU boundaries, but multinational cooperation also is an important part of the EU's external policies. Moreover, the EU could via enhanced the international cooperation and promote to establish a prevail global data transfer and protection framework to advance the EU's influence.

From another perspective to review the adequacy decision, although the adequacy decision request the third countries and regions provide the same level protection to the personal data as the precondition of the data transfer cross-border, it also means the EU through the adequacy decision to launch a negotiation with the third country and is equivalent to that EU evaluate the commercial relation with the third country. And that will push the other countries which cannot abandon the EU market to reformulate the domestic personal data protection laws to pursuit to make a consistent with the EU law, like Albania, Bolivia, Croatia, Macedonia, Andorra, and even the Russian respectively revised their regulations and laws.[252] Although the scramble for leading the development of personal data protection standards is also an approach for EU to consolidate its existing economic interests, the transplantation will inevitably be influenced by the receiving country due to political, cultural, economic, historical and other factors.[253] Since the EU established a high standard for the personal data protection system, if the EU is trying to carry out the whole system directly to other countries, the conflict on the values and other aspects will be inevitable. Therefore, the EU should propose and organise the international conference to pursuing establish a multilateral cooperation framework on personal data protection, with the cooperation and participation of more countries are not only more effective, they can

[252] Wugmeister, Miriam; Retzer, Karin, & Rich Cynthia, "Global Solution for Cross-border Data Transfers: Making the Case for Corporate Privacy Rules", *Springs*, 38 Geo. J. Int'l L.449, 2007.
[253] Baker, Mark B. "No country left behind: The exporting of US legal norms under the guise of economic integration." *Emory Int'l L. Rev.* 19 (2005): 1321.

significantly reduce the cost of important information collection, supervision, and enforcement agreements, but also through the establishment of multilateral cooperation framework and procedural rules to make member countries' decision-making and implementation mechanism more transparent, and the corporations could via those measures to improve their privacy policies be more accurate and stable.

The Global Privacy Enforcement Network (GPEN)[254], aim to promote cooperation among privacy enforcement authorities in privacy protection, is a wonderful example of the multilateral cooperation mechanism. However, as the announcements of the GPEN action plan, this project is not compulsory and the participants also no necessity to provide the confidential or sensitive information, it also not intended to interfere with government actions related to national sovereignty, civil and criminal law enforcement, national security, etc.[255] The GPEN cannot ensure each participant will comply and follow the decisions; besides, the progress of the GPEN is slowing down and faced several tough problems.[256] Therefore, the EU could go through other international organisation to establish a multilateral cooperation framework on the transborder data flow, and the WTO might be a suitable platform. The data only valuable when it connected with commercial services, and as the international organization which aims to promote the world trade, the international agreement of the transborder data flow still blanking in the WTO agenda. Hence, the WTO has an obligation to promote and establish the general world digital trade agreement and the relevant rules to regulate the cross-border data flow. Firstly, EU could propose to promote the addition of digital trade rules under existing WTO agreements, reform the classification system of trade goods to add the related digital trade clauses like cross-border data flow, privacy protection, and IP protection into the GATS, ITA, TRIPS, and TFA. Secondly, promote the establishment of a standing working committee to discuss international rules on digital trade under the WTO multilateral framework, the existing multinational digital trade rules could be samples for the proposal, like the CBPRs, the Privacy Shield, and the related provisions in the TTIP. Thirdly, the EU could propose to establish a special agreement for the world digital trade under the WTO framework, then submit the agreement proposal which based the EU standard and via the advantages of their comprehensive legal framework in the digital trade and privacy protection to lobby the member countries accept this

[254] The Global Privacy Enforcement Network (GPEN), available at: https://www.privacyenforcement.net .
[255] Global Privacy Enforcement Network, Action Plan for the Global Privacy Enforcement Network, available at: https://www.privacyenforcement.net/public/activities .
[256] Bennett, Colin. "The Global Enforcement Privacy Network: A Growing Network But How Much Enforcement?.", *Privacy Laws & Business International Report*, 137 (2015), pp. 19-21.

agreement. Obviously, this will be a tedious and tough work for the EU to pursue the leading position in the further digital economy in the world.

Bibliography

I. BOOKS

1. Bennett, Colin J. *Regulating Privacy: Data protection and public policy in Europe and the United States*. Cornell University Press, 1992.

2. Chalmers, Damian, Gareth Davies, and Giorgio Monti. *European union law*. Cambridge university press, 2019.

3. Greenwald, Glenn. *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. Macmillan, 2014.

4. Lynskey, Orla. *The foundations of EU data protection law*. Oxford University Press, 2015.

5. Kuner, Christopher. *European data protection law: corporate compliance and regulation*. Vol. 20. Oxford: Oxford University Press, 2007.

6. Manyika, James, et al. *Digital globalization: The new era of global flows*. Vol. 4. San Francisco: McKinsey Global Institute, 2016.

7. Moerel, Lokke. Binding corporate rules: corporate self-regulation of global data transfers. OUP Oxford, 2012.

II. JOURNALS/ PERIODICALS/ ARTICLES

8. Aaronson, Susan Ariel, and Patrick Leblond. "Another digital divide: the rise of data realms and its implications for the WTO." *Journal of International Economic Law* 21.2 (2018).

9. Ahmed, Mured, and Richard Waters. “Microsoft unveils German data plan to tackle US internet spying” *Financial Times* (2015).

10. Ahmed, Shahab. "A Discussion of Practical Steps to Harmonize Data Protection Rules Globally.", (2011).

11. Annas, George J., Leonard H. Glantz, and Patricia A. Roche. "Drafting the Genetic Privacy Act: science, policy, and practical considerations." *The Journal of Law, Medicine & Ethics* 23.4 (1995).

12. Assey Jr, James M., and Demetrios A. Eleftheriou. "The EU-US privacy safe harbor: smooth sailing or troubled waters." *CommLaw Conspectus* 9 (2001).

13. Baker, Mark B. “No country left behind: The exporting of US legal norms under the guise of economic integration.” *Emory Int'l L. Rev.* 19 (2005).

14. Bennett, Colin J. "The adequacy of privacy: The European Union data protection directive and the North American response." *The Information Society* 13.3 (1997): 245-264.

15. Bo Wang. "The Comments of the EU and the U.S ‘Safe Harbor Framework’ ." *Knowledge Economy* 4 (2013).

16. Cate, Fred H. "The EU data protection directive, information privacy, and the public interest." *Iowa L. Rev.* 80 (1994)

17. Choma, Alicja. "3.6. Big data–conditions of use and impact on business and society." *Quality. Central and Eastern Europe Focus*: 213.

18. Cunningham, McKay. "Privacy in the age of the hacker: balancing global privacy and data security Law." *Geo. Wash. Int'l L. Rev.* 44 (2012): 643.

19. Daoli Huang, and Zhile He, "'Big Data Phenomenon' of US and EU Data Cross-border Regulation Legislation and Enlightenment for China," *Journal of Intelligence* 4, 2017.

20. De Hert, Paul, and Serge Gutwirth. "Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action." *Reinventing data protection?*. Springer, Dordrecht, 2009.

21. De Hert, Paul, et al. "The right to data portability in the GDPR: Towards user-centric interoperability of digital services." *Computer Law & Security Review* 34.2 (2018).

22. Dwyer, A. C. "The NHS cyber-attack: A look at the complex environmental conditions of WannaCry." *RAD Magazine* 44 (2018).

23. Fang Ma. "The Existence and Abolition of the US-Europe Cross-Border Information 'Safe Harbor'." *China Information Security* 11 (2015).

24. Greenleaf, Graham. "Five years of the APEC Privacy Framework: Failure or promise?." *Computer Law & Security Review* 25.1 (2009).

25. Hondius, Frits W. "Data law in Europe." *Stan. J. Int'l L.* 16 (1980): 87.

26. Hong, Yanqing, and Ge, Xin, "Interpretation of National Standard 'Information Security Technology – Personal Information Security Specification'", *Secrecy Science and Technology*, 08 (2019).

27. Hornung, Gerrit, and Christoph Schnabel. "Data protection in Germany I: The population census decision and the right to informational self-determination." *Computer Law & Security Review* 25.1 (2009).

28. Hu, Wei, "Value Orientation and China's Choice on Transborder Data Flow", *Journal of Social Sciences*, 04 (2018).

29. Israel, Barbara A., et al. "Critical issues in developing and following CBPR principles." *Community-based participatory research for health: Advancing social and health equity*(2017).

30. Introna, Lucas D. "Privacy and the Computer: Why We Need Privacy in the Information Society." Metaphilosophy 28, no. 3 (1997): 259-75.

31. Jin, Jing. “An Overview of the General Data Protection Regulation-Evolution, Key Points and Major Issues” *Chinese Journal of European Studies* 4 (2018): 1.

32. Kamara, Irene, and Paul De Hert. "Data protection certification in the EU: Possibilities, actors and building blocks in a reformed landscape." *Privacy and data protection seals*. TMC Asser Press, The Hague, 2018. 7-34.

33. Kimery, Kathryn M., and Mary McCord. "Signals of trustworthiness in e-commerce: consumer understanding of third-party assurance seals." *Journal of Electronic Commerce in Organizations (JECO)* 4.4 (2006).

34. Kirby, Michael D. "Transborder Data Flows and the Basic Rules of Data Privacy." *Stan. J. Int'l L.* 16 (1980): 27.

35. Kuner, Christopher. "Regulation of transborder data flows under data protection and privacy law: past, present, and future." *TILT Law & Technology Working Paper* 016 (2010).

36. Kuner, Christopher. "Reality and illusion in EU data transfer regulation post Schrems." *German Law Journal* 18.4 (2017).

37. Liu, Jinrui, “Comments and Proposals regarding the Provision on the Security Assessment for Personal Information and Important Data to Be Transmitted Abroad (Draft)”, *Information Security and Communications Privacy*, 06 (2017).

38. Long, William J., and Marc Pang Quek. "Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise." *Journal of European Public Policy* 9.3 (2002).

39. Lucas D Introna, "Privacy and the Computer: Why We Need Privacy in the Information Society," *Metaphilosophy* 28, no. 3 (1997).

40. Mayer-Schönberger, Viktor, and Kenneth Cukier. *Big Data: A Revolution That Will Transform How We Live, Work and Think*. London: John Murray, 2013.

41. McKay Cunningham, “Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law,” *Geo. Wash. Int'l L. Rev.* 44 (2012).

42. Mengshan Ren, “The Information Space and Geographic Space: the Internet Communication and National Sovereignty,” *Modern Communication* (*Journal of Communication University of China*), 6, 2011.

43. Mulligan, Deirdre K. "Reasonable expectations in electronic communications: A critical perspective on the Electronic Communications Privacy Act." *Geo. Wash. L. Rev.* 72 (2003).

44. Ni Loideain, Nora. "The end of safe harbor: Implications for EU digital privacy and data protection law." *Journal of Internet Law* 19.8 (2016).

45. O’Connor, Brendan. “Quantifying the Cost of Forced Localization.” *Leviathan Security Group, June* (2015).

46. Ottis, Rain. "Analysis of the 2007 cyber-attacks against estonia from the information warfare perspective." *Proceedings of the 7th European Conference on Information Warfare*. 2008.

47. Penney, Jonathon W. "Chilling effects: Online surveillance and Wikipedia use." *Berkeley Tech. LJ* 31 (2016): 117.

48. Poullet, Yves. "EU data protection policy. The Directive 95/46/EC: Ten years after." *Computer Law & Security Review*22.3 (2006).

49. Qi, Aiming, "On the Improvement of the Comprehensive Legal Protection of Data Security in the Big Data Era——From the View of Cyber Security Law", *Journal of Northeast Normal University (Philosophy and Social Sciences)*, 04 (2017).

50. Qi, Aiming, & Pan, Jia, "Right to Data, Data Sovereignty and the Basic Principle of Big Data Protection", *Journal of Soochow University (Philosophy & Social Science Edition)*, 36 (2015).

51. Recio, Miguel. "Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability." *Eur. Data Prot. L. Rev.* 3 (2017).

52. Reding, Viviane. "Why the EU needs new personal data protection rules?." *The European Data* (2010).

53. Riccardi, J. Lee. "The German Federal Data Protection Act of 1977: Protecting the right to privacy." *BC Int'l & Comp. L.* Rev. 6 (1983): 243.

54. Roth, Paul. "Adequate Level of Data Protection in Third Countries Post-Schrems and under the General Data Protection Regulation." *JL Inf. & Sci.* 25 (2017).

55. Rudraswamy, Vanishree, and David A. Vance. "Transborder data flows: adoption and diffusion of protective legislation in the global electronic commerce environment." *Logistics Information Management* 14.1/2 (2001).

56. Simitis, Spiros. "From the market to the polis: The EU directive on the protection of personal data." *Iowa L. Rev.* 80 (1994): 445.

57. Tian, Xu. "Rising and reflection of data localization legislation", *Journal of Dalian Maritime University (Social Science Edition)*, 01 (2020).

58. Tian, Xu, A Step Forward Made by the US Cloud Act in Cross-Border Jurisdiction, *Journal of Customs and Trade*, 04 (2018).

59. Tourkochoriti, Ioanna. "The Snowden revelations, the Transatlantic Trade and Investment Partnership and the divide between US-EU in data privacy protection." *University of Arkansas at Little Rock Law Review* 36 (2014).

60. Voss, W. Gregory. "The Future of Transatlantic Data Flows: Privacy Shield or Bust?." *Journal of Internet*

Law 19.11 (2016).

61. Wagner, Julian. “The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?.” *International Data Privacy Law* (2018).

62. Wachter, Sandra. "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR." *Computer law & security review* 34.3 (2018).

63. Weiss, Martin A., and Kristin Archick. "US-EU data privacy: from safe harbor to privacy shield." (2016).

64. Wilson, Therese, Nicola Howell, and Genevieve Sheehan. "Protecting the most vulnerable in consumer credit transactions." *Journal of Consumer Policy* 32.2 (2009)

65. Wu, Weiguang, “Critique of Personal Data Protection Theory under Big Data Technology”, *Political Science and Law*, 07 (2016).

66. Wugmeister, Miriam; Retzer, Karin, & Rich Cynthia, “Global Solution for Cross-border Data Transfers: Making the Case for Corporate Privacy Rules”, *Springs*, 38 Geo. J. Int'l L.449, 2007.

67. Yong-qin, Gong, and Wang Jian. “Comparison of Cross-border Privacy Rules of APEC and EU.” *Asia-pacific Economic Review* 5 (2015).

68. Yue Shi, “The Management of Transborder Data Flow Under the Digital Economy,” *Information Security and Communications Privacy* 10, (2015).

69. Zhang YuAn and Song Kai, "Thoughts on the Risk of Cross-border Flow of Data in the New Period," *ZhongGuoXinXiAnQuan*, no. 11 (2018).

70. Zhang, Sheng, “The International Law Regulation Path of Cross-border Data Flows by the United States and China’s Countermeasures”, *Business and Economic Law Review* (04)2019.

71. Zhifang, Ji, “Research on the Legal Regulation of the Cross-border Flow of Personal Financial Information”, Huabei Finance, 08 (2015).

III. OTHER DOCUMENTS

72. Aiming Qi, The Legal Issues Research on Personal Information Protection Law and Transborder Data Flow, Wuhan University Press, 2004.

73. ALLEN, OVERY. "Binding Corporate Rules." May 2016.

74. Commission Staff Working Document, “On the Free Flow of Data and Emerging Issues of the European Data Economy”, *Accompanying the Document Communication Building a European Data Economy*, 10.01.2017, SWD (2017) 2 final.

75. China Internet Network Information Center, "*The 44th China Statistical Report on Internet Development*", Aug 2019.

76. Cui, Mengmeng, *Research on Legal Problems of Privacy Protection in Cross-border Data Flows*, East China University of Political Science and Law, 2019.

77. Dashboard, EU Cybersecurity. "A Path to a Secure European Cyberspace." (2014).

78. Economics, Oxford. "*Digital Spillover: Measuring the True Impact of the Digital Economy*." A Report by Huawei and Oxford Economics, Oxford, United Kingdom, (2017)

79. Eurobarometer, Special. "390-Cyber Security Report." Publication: July (2012); & EU Commission. "Special Eurobarometer 423: Cyber Security Report." (2015).

80. European Commission, "The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce," *SEC* (2004) 1323, 20 Oct. 20, 2004.

81. Kong Lingjie, *Legal protection of personal data privacy*, Wuhan University Press, 2009.

82. United States, Executive Office of the President, and John Podesta. *Big data: Seizing opportunities, preserving values. White House, Executive Office of the President*, 2014.

IV. CASE LAW

1. Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015, ECLI:EU:C:2015:650.

2. Joined Cases C-203/15 and C-698/15, Tele2 Sverige & Secretary of State for the Home Department, ECL:EU:C:2016:970, 21 December 2016.

V. LEGAL INSTRUMENTS

A. EU

A.1 Binding

3. Council of European Union, *Convention for the Protection of Human Rights and Fundamental Freedoms*, ETS 5, 4 November 1950.

4. Council of European Union, Parliamentary Assembly Recommendation 509, *Human Rights and Modern Scientific and Technological Developments*, 31 January 1968.

5. European Commission, the Communications from the Commission to the Council, *Community policy on data processing. Communication of the Commission to the Council. SEC (73) 4300 final*, 21 November 1973.

6. European Commission, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", European Treaty Series no. 108, January 28, 1981.

7. 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, *OJ* L 281, 23 November 1995.

8. European Commission, Standard contractual clauses for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to third countries which do not ensure an adequate level of protection, (2001).

9. European Commission, Commission Decision C (2004)5721 SET II Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers) (2004).

10. Directive (EC) 2002/58/EC of the European Parliament and of the Council of 12 July 2002, *concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, OJ L 201, 31 July 2002

11. Directive (EU) 2010/13/EU of the European Parliament and of the Council of 10 March 2010, *on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)*, OJ L 95, 15 April 2010.

12. Communication from the Commission. "A Comprehensive Approach on Personal Data Protection in the European Union." *COM (2010)* 609 (2010).

13. Treaty (EU) C 326/391, *Charter of Fundamental Rights of the European Union*, *OJ* C 326, 26 Oct 2012.

14. European Commission, *2013/65/EU: Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand (notified under document C (2012) 9557) Text with EEA relevance*, *OJ* L 28, 30 January 2013.

15. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (*General Data Protection Regulation*) (*Text with EEA relevance*), *OJ* L 119, 4 May 2016.

16. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, *concerning measures for a high common level of security of network and information systems across the Union*, OJ L 194, 19 July 2016.

17. Decision (EU) 2016/1250, *pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, *OJ* L 207, 1 August 2016.

A.2 Non-binding

18. European Commission, Commission Recommendation of 29 July 1981 Relating to the Council of Europe

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, OJ L 246, 29 August 1981.

19. Council of the European Union, *Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data*, COM (1990) 314-2, *OJ* C 277, 5 November 1990.

20. European Commission, Data Protection Working Party, WP4: *First orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy*, XV D/5020/97-EN final, 26 June 1997.

21. European Commission, Data Protection Working Party, WP12: *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, DG XV D/5025/98, 24 July 1998.

22. European Commission, Data Protection Working Party, *WP107: Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules"*, 14 April 2005.

23. European Commission, Data Protection Working Party, *WP 153: Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*, 24 June 2008.

24. European Commission, Communication from the Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final, 7 February 2013.

25. European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A Digital Single Marker Strategy for Europe*, COM (2015) 192 final, 6 May 2015.

26. European Commission, "Why we need a Digital Single Market," *Factsheets on Digital Single Market*, 6 May 2015.

27. Article 29 Data Protection Working Party, Article 29 Working Party Guidelines on consent under Regulation 2016/679, WP259 rev.01, 28 Nov 2017.

B. U.S.

28. U.S. Congress, *The first 10 amendments form the Bill of Rights*, Dec 15, 1791.

29. The Act of United State, *Privacy Act of 1974*, 5 U.S.C. § 552a.

30. The Act of United State, *Electronic Communications Privacy Act of 1986 (ECPA)*, 18 U.S.C. §§ 2510-2523.

31. The Act of United State, *The Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507 (1988), amended the Privacy Act of 1974*, 5 U.S.C. § 552a.

32. United States. White House Office. *A framework for global electronic commerce*. White House, 1997.

33. Swiss and United States, Swiss-US Privacy Shield: better protection for data transferred to the USA.

34. United States Federal Trade Commission, “Privacy & Data Security Update” (2017).

35. The Act of United States, *the Clarifying Lawful Overseas Use of Data (CLOUD) Act*, (2018) H.R.4943.

C. APEC

36. Asia-Pacific Economic Cooperation, "APEC Privacy Framework," *Asia Pacific Economic Cooperation Secretariat* 81 (2005).

37. Asia-Pacific Economic Cooperation, “*APEC Data Privacy Pathfinder Projects Implementation Work Plan*”, 2009/SOM1/ECSG/SEM/027.

38. Asia-Pacific Economic Cooperation, “*The APEC Cross-border Privacy Enforcement Arrangement (CPEA)*”, 2010/SOM1/ECSG/DPS/013.

39. Asia-Pacific Economic Cooperation, “Cross Border Privacy Rules and Privacy Recognition for Joint Oversight Panel”, 19 Feb 2013, as amended 18 June 2013.

40. Asia-Pacific Economic Cooperation, “*APEC Cross-Border Privacy Rules System, Policies, Rules and Guidelines (Updated as of November 2019)*”.

D. CHINA

41. People’s Bank of China, “*Notice by the People’s Bank of China Regarding the Effective Protection of Personal Financial Information by Banking Institutions*”, No.17 (2011) of the People's Bank of China, 21 Jan 2011.

42. Inspection and Quarantine and the Standardization Administration of China, “*Information Security Technology - Guidelines for the Protection of Personal Information in Public and Commercial Service Information Systems*”, GB/Z 28828-2012, 5 Nov 2012.

43. State Council of China, “*Regulation on the Administration of Credit Investigation Industry*”, No.631 Order of the State Council, 21 Jan 2013.

44. State Council of China, “*Outline of the 13th Five-Year Plan for the National Informatization*”, No.73 (2016) Order of the State Council, 15 Dec 2016.

45. Standing Committee of the National People’s Congress of China, “*Cybersecurity Law of China*”, No.53 Order of the President of the People's Republic of China, 1 June 2017.

46. Cyberspace Administration of China, “*Security Assessment for Personal Information and Important Data to Be Transmitted Abroad (Draft for comments)*”, 11 Apr 2017.

47. Standardization Administration of China, “*Information Security Technology – Personal Information Security Specification*”, GB/T 35273-2020, 6 Mar 2020.

E. OTHERS

48. Germany, Hessisches Datenschutzgesetz, (Hessen Data Law), 7 October 1970.

49. OECD, "Policy Issues in Data Protection and Privacy," *OECD Informatics Studies*, No. 10, OECD, 1974.

50. OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)".

51. The Global Privacy Enforcement Network (GPEN), available at: https://www.privacyenforcement.net .

VI.WEBSITES

European Commission, *Adequacy decisions-How the EU determines if a non-EU country has an adequate level of data protection*, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en .

European Commission, "Europe 2020 strategy," available at: https://ec.europa.eu/digital-single-market/en/europe-2020-strategy .

European Commission, "Shaping the Digital Single Market," available at: https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market .

European Commission, "BCR overview until 25th May 2018." 25 May 2018, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en .

European Commission, Collecting & processing personal data: what is legal?, available at: http://ec.europa.eu/justice/data protection/data-collection/legal/index_en.htm .

The Online Privacy Alliance of United States, *Privacy Alliance*, available at: http://www.privacyalliance.org .

Asia-Pacific Economic Cooperation, "*About CBPR*", available at: http://cbprs.org/about-cbprs/ .

Asia-Pacific Economic Cooperation, "*CBPR Intake Questionnaire*", available at: https://cbprs.blob.core.windows.net/files/Cross%20Border%20Privacy%20Rules%20Intake%20Questionnaire.pdf .

Global Privacy Enforcement Network, Action Plan for the Global Privacy Enforcement Network, available at: https://www.privacyenforcement.net/public/activities .

iiMedia Research, "*2018-2019 China Cross-border E-commerce Market Research Report*", 22 Mar 2019, available at: https://www.iimedia.cn/c400/63893.html .