The Regulation of Transborder Data Flows

from the EU to China Within the Framework of

China-EU E-Commerce under the GDPR

Dissertation
zur Erlangung des Doktorgrades
der juristischen Fakultät
der Georg-August-Universität zu Göttingen

von

Lu Yu
aus Hunan, China

Göttingen, 2023

Table of Content

Abstract.....VII

Chapter 1 Data Flow from the EU to China Under the Framework of EU-China Cross-border E-Commerce.....1

I. Introduction..... 1

1. Background and research question..... 1

2. Research methods..... 4

2.1 Case study..... 4

2.2 Comparative study..... 4

II. Definition of Cross-border E-Commerce and Volume of China-EU Cross-border E-Commerce 5

1. Definition of cross-border E-Commerce..... 5

2. Different models of cross-border E-Commerce businesses..... 5

2.1 Cross-border E-Commerce per own website or App..... 6

2.2 Cross-border E-Commerce via third party platform..... 7

III. Transborder Data Flows in Different Scenarios Within the Framework of China-EU Cross-border E-Commerce.....11

1. Data flows from an EU controller to a Chinese controller or processor.....11

2. Data flows from the EU to China without an EU established controller..... 12

2.1 Personal data directly transferred by an EU data subject to a Chinese data controller .. 12

2.2 Personal data transferred from an EU processor to a Chinese controller..... 13

Chapter 2 Extraterritorial Application of the GDPR and its Problems 15

I. Art. 3: Territorial Scope of the GDPR 16

1. Controllers or processors with data processing relevant establishment in the EU 16

1.1 Establishment 17

1.2 Processing carried out in the context of the activities of the establishment 20

1.3 Practical significance for cross-border E-Commerce operators 22

2. Controllers or processors without data processing relevant establishment in the EU 23
2.1 From making use of equipment situated on the territory of EU to the marketplace principle 23
2.2 Processing related to the offering of goods or services to data subjects in the EU 25
2.3 Processing related to the monitoring of behavior of the EU data subjects 26
2.4 Application to cross-border E-Commerce operators 27
II. Jurisdictional Controversy Regarding the Territorial Scope of the GDPR per Art. 3 28
1. Extraterritoriality under public international law 29
1.1 Jurisdiction 29
1.2 Extraterritorial jurisdiction 31
2. Extraterritoriality of the GDPR 37
3. Brief summary 39
III. Possibilities to Enforce the GDPR in China 40
1. Public and private enforcement possibilities under the GDPR 40
1.1 Private Enforcement possibilities under the GDPR 41
1.2 Public enforcement of the GDPR 44
2. Recognition and enforcement of foreign civil and commercial judgements in China 46
2.1 Recognition and enforcement based on mutual judicial assistance treaties 47
2.2 Recognition and enforcement in accordance with the principle of reciprocity 48
2.3 Brief summary 50
3. Administrative investigation and enforcement actions by the data supervisory authority in China 51
4. Alternative: market destruction measures 51
5. Mid-conclusion 53

Chapter 3 The Concept and Legal Basis of Data Transfer under the GDPR 55

I. The Definition of Data Transfer Within the Meaning of Chapter V GDPR 55
1. Transfer: the act element 56
2. The intention to disclose personal data to recipients in a third country 59
3. The transferor and recipient 59
3.1 Data controller as transferor: controller to controller and controller to processor 60

3.2 Data processor as transferor: processor to controller or processor to sub-processor..... 62
3.3 Transfer directly by the data subject to a recipient outside of the EU 65
II. Behind the Dispute of Opinions: The Relationship Between Art. 3 (Application Scope) and Chapter V (Data Transfer Rules)..... 68
III. Data Transfers from the EU to a Third Country or International Organization .. 71
1. Adequacy decision..... 73
1.1 Core contents of the data protection material rules 74
1.2 Enforcement mechanism 75
1.3 Rules concerning data access by public authorities for law enforcement and national security purposes 76
2. General about the appropriate safeguards 78
2.1 Accountability of the parties involved in the transfer 78
2.2 Enforceable data subject rights..... 79
2.3 Effective legal remedy for data subjects..... 80
2.4 Type of the appropriate safeguards and respective conditions 80
2.5 High requirements on appropriate safeguards after "Schrems II"..... 90
2.6 Derogations from the adequate protection..... 98
IV. Features and Functions of the Data Transfer Rules Compared to the Direct Application of GDPR 99
1. The enforcement problem arising from the application of Art. 3 100
1.1 Adoption and enforcement of appropriate safeguards..... 101
1.2 Stricter conditions required by the derogations..... 102
2. The subjection of the non-EU data controller to the law of the third country..... 103
3. Mid-conclusion..... 104

Chapter 4 Data Protection Level in China in Comparison to the EU 105

I. Global Data Protection and Data Protection Development in China..... 105
1. Global data protection trend 105
2. Data protection development in China 107
2.1 Data protection as a fundamental right in China? 108
2.2 Influence of the fundamental right approach in China 111
II. Substantial Data Protection Rules in China.....113

1. Data protection in the Civil Code 113
1.1 Protection of the personal data – a right or legally protected interest? 114
1.2 Impact of the introduction of the protection of personal data in the Civil Code 116
2. Data protection under the Cybersecurity Law 117
2.1 Principles for data collection and use 119
2.2 Rights of the data subject 121
2.3 Obligations of the network data controller 122
2.4 Data protection supervisory authority 122
2.5 Administrative and judicial remedy 123
3. Data protection in consumer law 126
3.1 Rules with regard to the protection of consumer personal data 126
3.2 Supervisory authority for the consumer data protection 127
4. Data protection in criminal law 128
5. The Personal Information Protection Law 130
5.1 Data processing principles, rights of the data subjects and obligations of the data controllers 131
5.2 The regulation of data processing activities carried out by public authorities 132
5.3 Supervision and enforcement 137
5.4 Remedies and liabilities 139
5.5 Brief summary 143
III. Access of Personal Data by Public Authorities for Purposes of Law Enforcement and National Security in China 147
1. General legal framework 147
2. Access by public authorities for criminal law enforcement purposes 149
2.1 Compulsory investigation and evidence collection 149
2.2 Supervision of the compulsory investigation and collection of electronic data 151
2.3 Judicial remedy for data access for the purposes of criminal law enforcement 152
3. Access by public authorities for national security purposes 153
3.1 Compulsory investigation for national security purposes 153
3.2 Supervision of compulsory investigations for national security purposes 154
3.3 Judicial Remedy for illegal data access for the purposes of national security 155
3.4 Brief summary 155
IV. Conclusion: Data Protection Level in China – is an Adequacy Decision About China

Possible? 156
1. The substantial data protection rules drawing close to the GDPR 157
2. The right of the data subject to administrative remedy and judicial remedy..... 158
3. The lack of effective implementation and enforcement of the substantial rules 159
4. The wide access of personal data by public authorities for the purpose of criminal law enforcement and national security..... 160

Chapter 5 Data Transfers Based on Appropriate Safeguards and Derogations 162

I. Data Transfers from an EU Based Data Controller to a Chinese Controller or Processor 162
1. EU established E-Commerce platforms transferring personal data to Chinese sellers... 162
1.1 Standard Contractual Clauses..... 163
1.2 Derogations..... 168
2. EU established E-Commerce platforms or sellers transferring personal data to Chinese service providers..... 170
II. Data Transfers from the EU to non-EU Data Controllers Subject to the GDPR per Art. 3 170
1. Data transfer from EU data processors to Chinese controllers that are subject to the GDPR per Art. 3..... 172
1.1 Binding corporate rules 173
1.2 Standard contractual clauses..... 173
1.3 Codes of conduct and data protection certification as appropriate safeguards for data transfers from EU processors to controllers in a third country..... 176
1.4 Derogations..... 184
2. Data transfers from EU data subjects to Chinese controllers 185
2.1 Applicability of the standard contractual clauses and binding corporate rules 186
2.2 Applicability of the codes of conduct and certifications 186
2.3 Applicability of the derogations 187
III. Brief summary..... 189

Chapter 6 Summary and Conclusion.....193

Bibliography 203

I. Literature..... 203

II. Positions, Opinions and Guidelines of data protection authorities..... 214

III. Case Law..... 216

IV. Internet Source 218

Abstract

With the promulgation of the General Data Protection Regulation, the protection of personal data in the EU has reached a historically high level. However, the EU cannot keep the personal data of its residents inside of the EU. Personal data of the EU data subjects are processed by and transferred to controllers or processors outside of the EU. The GDPR tries to regulate such transborder data flows by applying its data protection rules extraterritorially and laying down stringent rules for data transfers from the EU to third countries.

This dissertation focuses on the data flows from the EU to China within the China-EU cross-border E-Commerce. It examines the applicability of the data transfer rules contained in the GDPR to such data flows as well as its impact and problems in the practice. The dissertation starts with an identification of the main scenarios of the transborder data flows from the EU to China. It then explores the territorial application scope of the GDPR according to Art. 3, examining whether and how the GDPR applies to such transborder data flows. After that, it scrutinizes the definition of data transfer within the meaning of Chapter V GDPR. Based on this definition, it goes on to analyze whether the data flow scenarios arising from the China-EU cross-border E-Commerce constitute a data transfer, and how Art. 3 and Chapter V GDPR should be applied, whether mutually exclusive or simultaneously. Further, if Chapter V GDPR does apply, what legal basis can be relied on to carry out the data transfer and what kind of obstacles exist.

Chapter 1 Data Flow from the EU to China Under the Framework of EU-China Cross-border E-Commerce

I. Introduction

1. Background and research question

In an era characterized by internet and globalization, data protection has become an unavoidable topic. With the General Data Protection Regulation ("GDPR")[1] entering into force on 25 May 2018, the protection of personal data in the EU reached a historically high level. However, the EU cannot keep the personal data of its residents inside the EU with a closed door. Personal data of EU residents are inevitably processed by controllers or processors outside of her jurisdiction as well as transferred to third countries in a globalized context. It is also a common practice for companies to collect and process personal data of the EU data subjects in third countries to circumvent the strict European data protection law. This raises the question whether the personal data of EU data subjects can be effectively protected in third countries. The EU tries to solve the above-mentioned problem by, among others, applying its data protection regulations extraterritorially and laying down specific rules regulating data transfers from the EU to third countries. However, the practical effect of this extraterritorial application of the EU data protection law is questioned. This is particularly the case with respect to Chinese companies. While there have been influential data protection enforcement actions against large American corporate groups in the recent years, and the EU and the U.S. have tried to reach data protection cooperation mechanisms, the application of data protection rules to Chinese companies and data transfers from the EU to China have received less attention than it deserves.

Along with China's rise as a global manufacturing power, Chinese small- and middle-sized sellers are expanding abroad with the help of internet. Moreover, to avoid an overreliance on giant American E-Commerce platforms, Chinese E-Commerce

[1] 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).

platforms have seized the chance to expand into the European market. The China-EU cross-border E-Commerce has experienced a surge in recent years. According to the official statistic of the Chinese government, from 2012 to 2017, China's cross-border E-Commerce managed an annual growth of about 30%.[2] As of 2012, the trading amount achieved through E-Commerce only accounted for 8.6% in China's total cross-border trading amount, by 2017, the trading amount by means of cross-border E-Commerce went up to 30% of the total cross-border trading volume.[3] In terms of the E-Commerce export destination, the US remains the largest export destination with 17.2% of the cross-border trading volume, closely followed the EU with 16.3% the second biggest export destination.[4] According to a survey carried out by the International Post Corporation in 2019 concerning cross-border E-Commerce in 41 countries (the majority of them are European countries), 39% of the cross-border parcels came from China.[5] In the majority of European countries, online shoppers do most of their purchasing from China.[6] The survey clearly showed that China is the leading E-Commerce exporter worldwide for successive years.[7]

Due to the booming cross-border E-Commerce business, a large amount of personal data of the EU data subjects flows across the EU border to China. In contrast to the booming transactions in cross-border E-Commerce, there is less attention in terms of the regulation of transborder E-Commerce. Even in the rather strict tax law area, Germany did not revise its law to prevent evasion of value-added tax with regard to the cross-border trade of goods on the internet until 2018. In terms of data protection, focus has largely been put on search engines and social media, more specifically on the American giants. Since very little clarification has been given to the data protection situation under the framework of the China-EU cross-border E-Commerce, and the huge cultural and linguistic barriers do not exactly contribute to a precise understanding of the scatted and constantly renewed Chinese data protection rules, users in the EU face a big problem of not knowing whether and how their data are sufficiently protected

[2] http://history.mofcom.gov.cn/?newchina=跨境电商蓬勃兴起, last visited on 08.02.2020.
[3] Ibid.
[4] Ibid.
[5] Cross-border E-Commerce Shopper Survey 2019 (public version), International Post Corporation, available at https://www.ipc.be/services/markets-and-regulations/cross-border-shopper-survey, last visited on 09.02.2020.
[6] Ibid.
[7] Ibid.

by the overseas Chinese sellers and platforms.

The promulgation of GDPR, indeed, has raised alarm among cross-border businesses. Particular attention has been paid to Chapter V GDPR which regulates the transfer of personal data to a third country or organization, since it seems to be the most relevant rules that would potentially apply to transborder data flows. Some international negotiations concerning data transfers from the EU to a third country, such as the "Privacy Shield" negotiation between the EU and the USA and the adequacy negotiation between the EU and Japan, have made the need for rules for data transfers to a third country or international organization even more evident. While it is absolutely necessary to adhere to the rules for data transfer to a third country, since the EU data protection law has imposed strict conditions on such data transfers and the violation of such rules could do harm to the cross-border business involved, it is not always clear what constitutes a data transfer to a third country. Specifically, it is not clear whether the common transborder data flows under the framework of cross-border E-Commerce all constitute a "data transfer" in the sense of Chapter V GDPR, further leading to the question whether the conditions laid down in Chapter V GDPR have to be complied with when such transborder data flows take place.

What is often ignored is that, in addition to the rules regarding data transfer to a third country or international organization, there are other rules in the GDPR that also deal with transborder data flows, namely Art. 3 GDPR regulating the territorial scope of the GDPR. If a data processing meets the conditions set out in Art. 3, the GDPR applies directly to that data processing. This is also the case even if data controllers or processors are located outside of the EU. However, the application of Art. 3 is also highly controversial due to the abstractness and vagueness of some of its key elements. Beyond the complexity of Art. 3 and Chapter V GDPR within themselves, it is also ambiguous how these two sets of rules interact with each other.

Therefore, this dissertation will, as a first step, define the main scenarios of the transborder data flows from the EU to China. It will then explore the territorial application scope of the GDPR according to Art. 3, examining whether and how the GDPR applies to the transborder data flow scenarios arising from the China-EU cross-border E-Commerce. After that, it will focus on the definition of data transfer within

the meaning of Chapter V GDPR. Based on this definition, it will go on to analyze whether the data flow scenarios arising from the China-EU cross-border E-Commerce constitute a data transfer, and how Art. 3 and Chapter V GDPR should be applied, whether mutually exclusive or simultaneously. Further, if Chapter V GDPR does apply, what legal basis can the parties rely on to carry out the transfer and what kind of problems will they face. In the end, a concluding remark will be made in terms of whether the fundamental right of the EU data subject concerning their personal data is sufficiently protected, when such personal data is sent from the EU to China in the course of China-EU cross-border E-Commerce.

2. Research methods

2.1 Case study

In a legal field in which numerous concepts are abstractly defined or even not defined at all, such as data protection law, case study is a useful tool that helps to contextualize general terminology and interpret legal provisions in a correct way. In this dissertation, special attention will be paid to the case law of the Court of Justice of the European Union ("CJEU"), since the CJEU's judgement ensures a uniform interpretation of the data protection law in all Member States of the EU.

2.2 Comparative study

Since the EU-China data transfer as well as the protection of personal data of EU data subjects in China is the focus of this dissertation, a detailed study of the Chinese data protection legal system is necessary. More specifically, the Chinese data protection rules will be analyzed in the light of the EU data protection standards, in order to assess whether China provides a level of data protection essentially equivalent to that of the EU.

II. Definition of Cross-border E-Commerce and Volume of China-EU Cross-border E-Commerce

1. Definition of cross-border E-Commerce

Electronic commerce ("E-Commerce") is used widely in various policy documents and legal contexts. However, there is no universal agreed definition about the term. While EU law does not provide a legal definition of E-Commerce, the Chinese E-Commerce Law defines E-Commerce as "business activities of selling commodities or providing services through the internet or any other information network"[8]. Based on this, cross-border E-Commerce can be defined in this dissertation as "business activities of selling commodities or providing services through the internet or any other information network cross national borders". Cross-border E-Commerce is sometimes also called international E-Commerce.[9]

This definition of E-Commerce shows several aspects that are noteworthy. Firstly, it suggests that in cross-border E-Commerce business, sellers and buyers are not located in the same country or jurisdiction region (such as the EU). Secondly, it involves the provision of both goods and services. Thirdly, the provision of goods or services must happen via internet or other information networks, whether it is per website or cellphone is irrelevant.

In connection with the above-mentioned definition of cross-border E-Commerce, China-EU cross-border E-Commerce in this dissertation refers to Chinese sellers selling commodities or providing services to EU consumers per internet, either through an E-Commerce platform or through own websites or mobile applications (apps). To this extent, both the activities of the sellers as well as that of the E-Commerce platform operators will be discussed.

2. Different models of cross-border E-Commerce businesses

Numerous classifications for E-Commerce exist. They are based respectively on

[8] Art. 2 of the E-Commerce Law of the People's Republic of China.
[9] See http://www.crossborder-ecommerce.com/international-expansion/, last visited on 11.02.2020.

different classification criteria, for example partial E-Commerce or pure E-Commerce, business–to-business E-Commerce or business-to-consumer E-Commerce.[10] The most relevant class in terms of data protection is, depending on whether a third-party platform is involved, E-Commerce through an established third-party platform (sales with intermediaries) or through the seller's own websites or apps (sales without intermediaries). From a data protection point of view, this difference directly relates to the question of how many stakeholders are involved in the data processing operations and who is the data controller for which data processing operation.

To gain a clear image of the typical data processing operations in the process of E-Commerce, it might prove helpful to consider, first, what kind of data are collected. Personal data that could possibly be collected by sellers, platform operators or third service parties usually include: a) order data indicating who bought what products or services, b) delivery data including name, address, phone number, c) payment data such as a credit card number, and d) other behavioral data such as search history, IP address, browsing time etc.[11] In most cases, some data are given actively by the user, such as name, address and phone number when registering for a personal account or issuing an order, whereas other data are collected rather cryptically via data collection tools that are inserted in the shopping website, such as cookies, web bugs, of which the user is not always aware. In the latter case, the categories and scope of the data collected are determined by the owner of the website and/or other entities that are authorized by the owner of the website. Thus, from the data collection perspective, it is essential to ascertain the owner of the E-Commerce website, since the owner of the website is frequently the controller or at least the joint-controller for the data processing operations during the visit of the website.

2.1 Cross-border E-Commerce per own website or App

In the case that a seller provides commodities or services per its own website or app, the seller is usually the owner or actual operator of the website or app, who determines

[10] TURBAN, Efraim; WHITESIDE, Judy; KING, David; OUTLAND, Jon, Introduction to Electronic Commerce and Social Commerce. Springer, 2017, part 1.
[11] ANTONIOU, Giannakis; BATTEN, Lynn, E-Commerce: Protecting Purchaser Privacy to Enforce Trust. Electronic Commerce Research, 2011, Vol. 11, pp. 421-456.

the purposes and means of the processing of personal data collected. This makes the seller the data controller. The seller may also have entrusted a specialized data processing company to deal with the technical dimensions of the data processing, which in principle works as a data processor following the obstructions of the data controller. In addition, the seller will most probably also engage other third-party service providers such as a payment service provider or an advertisement service provider in the online business, these service providers may be data processors if they only process the user's personal data for the seller.

An example of providing products or services per own website from China is the cellphone provider OnePlus. The Chinese company based in Shenzhen not only has webstores in major E-Commerce platforms, but also sells its products directly per own website to European consumers. Their privacy policy states that the China-based based OnePlus Technology (Shenzhen) Co., Ltd. is the designated data controller for the personal data processed in the scenario where the privacy policy is showed or linked to.[12] Beyond that, a variety of Chinese travel agencies and language schools also have online presence or apps oriented towards European users.

2.2 Cross-border E-Commerce via third party platform

For small or medium-sized sellers, trading on an E-Commerce platform is an ideal way to provide goods or services to customers, especially to customers abroad. Since it is rather cost intensive to do direct advertisement in foreign countries, local and international platforms have the advantage of having existing clients on the local market, many of them also provide payment and logistic supports, which solves some of the biggest problems for cross-border E-Commerce traders. While traders profit from platforms, platforms also profit from traders, since it is the offers of the traders that attract consumers and their transactions and communications with the consumer that generates numerous data, which the platforms then use for their own purposes.[13]

[12] Privacy Policy of ONEPLUS (English version), available at https://www.oneplus.com/de/legal/privacy-policy, last visited on 12.02.2020.
[13] DEMARY, Vera, et al, Data Sharing im E-Commerce— Legal and Economic Basics (Rechtliche und ökonomische Grundlagen). Gutachten für ServiCon Service & Consult eG, 2019.

Generally, there is no universally recognized definition of E-Commerce platform. In connection with the OECD's policy documents which deal with E-Commerce and E-Commerce platforms, we can consider E-Commerce platforms as platforms that bring sellers and buyers together without being a party of the transaction.[14] Some platforms are only marketplaces that provide trading infrastructure for buyers and sellers, while others may also sell their own products at the same time (such as Amazon). However, websites that only sell their own products shall not be deemed as E-Commerce platforms, since it does not function as a marketplace for other traders. Also, according to the definition of E-Commerce and E-Commerce platforms adopted in this dissertation, online platforms that do not bring sellers and buyers together in order to complete a transaction are not E-Commerce platforms, such as pure search engines, social media, communication platforms, which are online platforms but not E-Commerce platforms.[15]

Though the services and functions of different E-Commerce platforms may vary, E-Commerce platforms generally collect a variety of personal data concerning both the seller and the buyer, since they technically run the website and organizationally handle the transactions.[16] Compared to sellers trading on a platform, the operator of a platform has access to much more personal data, in particular data concerning the users. Research of the OECD regarding online platforms reveals that online platforms usually collect personal identification data, payment data, product transaction data, personal expression data, browsing data, device and connection data, location data.[17] These data are either provided by the users, or observed form the users' behavior.[18]

Another question is how E-Commerce platforms interact with sellers in terms of the collection and transfer of personal data concerning buyers. It has to be noted that not only E-Commerce platforms but also sellers collect personal data concerning buyers.

---

[14] OECD, Unpacking E-Commerce: Business Models, Trends and Policies, OECD Publishing, Paris, 2019, available at https://doi.org/10.1787/23561431-en, last visited on 15.02.2020.

[15] Classification of online platforms see, Background Paper of the Bundeskartellamt's Working Group on Competition Law, Digital Economy - Internet Platforms Between Competition Law, Privacy and Consumer Protection (Hintergrundpapier des Arbeitskreises Kartellrecht des Bundeskartellamts, Digitale Ökonomie – Internetplattformen zwischen Wettbewerbsrecht, Privatsphäre und Verbraucherschutz), https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Diskussions_Hintergrundpapier/AK_Kartellrecht_2015_Digitale Oekonomie. html, p. 8-9, last visited on 16.02.2020.

[16] OECD, An Introduction to Online Platforms and Their Role in the Digital Transformation, OECD Publishing, Paris, 2019, available at https://doi.org/10.1787/53e5f593-en, p. 68, last visited on 16.02.2020.

[17] Ibid.

[18] Ibid.

This is the case, for example, when a buyer launches a communication or concludes a transaction with a seller. Such data directly needed for or related to a specific transaction may be either transferred by the platform to the seller, or directly provided by the buyer. In such cases, the seller is also the data controller for the data processing. However, personal data collected by the seller in the above scenario are not comparable in scope to that collected by platforms. Not only do platforms collect the above transaction data, but they collect it on massive proportions, beyond that, the browsing and behavior data are collected only by platforms through various trackers.[19] The latter are usually only under the control of platforms, to which sellers will not be granted access.[20] For the processing of such data, the E-Commerce platform is the data controller, whereas other third-party service providers such as advertisement companies or data analysis experts may work as data processor for the E-Commerce platform.

In consideration of the dominant role of the E-Commerce platform in data processing, and the scope of this dissertation concerning EU-China cross-border data transfer, it is necessary to draw a difference between the non-Chinese E-Commerce platforms and the Chinese E-Commerce platforms on the EU market, on which the Chinese sellers are active.

2.2.1 Non-Chinese cross-border E-Commerce platforms on the EU market

Nowadays, Chinese sellers are active almost on every major E-Commerce platform. A study in 2017 of the Marketplace Pulse, which is an E-Commerce intelligence firm according to its own resource,[21] found that 25% of the sellers on the 5 European Amazon marketplaces are based in China[22]. Moreover, another study from the same firm revealed that at least 40% of the new sellers from 2017 to 2018 in the Amazon European marketplaces originate from China.[23] This illustrates the huge expansion of China-EU cross-border E-Commerce and makes the need for a legal investigation of

[19] DEMARY, Vera, et al, Data Sharing im E-Commerce— Legal and Economic Basics (Rechtliche und ökonomische Grundlagen). Gutachten für ServiCon Service & Consult eG, 2019.
[20] Ibid, p. 6.
[21] https://www.marketplacepulse.com/about, last visited on 17.03.2020.
[22] https://www.marketplacepulse.com/articles/china-share-of-amazon-marketplace-is-likely-as-much-as-25-percent, last visited on 17.03.2020.
[23] https://www.marketplacepulse.com/articles/one-million-new-sellers-on-amazon, last visited on 17.03.2020.

the occurring data flows even more evident and timely.

Not only Amazon, but also in other international E-Commerce platforms that are popular in Europe, such as eBay and Wish, Chinese sellers make up a large proportion. Noteworthy is Wish, which focuses on low price products made in China. According to Marketplace Pulse, the Wish shopping app is one of the most popular shopping apps downloaded in the EU.[24] From the author's own experience, Wish is particularly popular among young people, including teenagers.

Reviewing the privacy policies of these non-Chinese E-Commerce platforms, it can be found that the above mentioned three E-Commerce platforms all have their headquarters in the US, however, they have designated a data controller in the EU for the processing of personal data concerning to EU data subjects. These privacy policies also state that they may transfer personal data to sellers or other service providers located in third countries for the purpose of fulfillment of the sales contract, which, of course, also includes sellers and service providers located in China.

2.2.2 Chinese E-Commerce platforms on the European market

Besides giant American E-Commerce platforms, there are also China-based E-Commerce platforms active on the European E-Commerce market. Consequently, these platforms focus on selling products or services from China to the EU, sellers on these platforms are mostly based in China.

The two best examples of Chinese based cross-border E-Commerce platforms active on the European market are AliExpress under the Chinese E-Commerce giant Alibaba and Joybuy held by another Chinese E-Commerce giant JD. AliExpress as a B2C cross-border E-Commerce platform together with the B2B platform Alibaba.com from the same business group has been popular in Europe more than a decade. This dissertation will focus on these two platforms as a case group.

In Europe, AliExpress has multi-language sites, such as sites in English, German,

[24] https://www.marketplacepulse.com/marketplaces-year-in-review-2018#wish, last visited on 17.05. 2020.

Spanish, Portuguese, Italian and Dutch. Its privacy policy, however, remains the same (English version) for all language sites.[25] It states that for users based in the EU, the data controller is Alibaba.com Singapore E-Commerce Private Limited, a company registered in Singapore, and that the relevant personal data will be stored in Germany.[26] Likewise, Joybuy also has English and Spanish language sites for business operations in Europe. Orders can be delivered to other European countries such as Germany, France, Greece and the Netherlands.[27] From Joybuy's privacy policy it can be seen that the data controller for processing of personal data concerning users visiting Joybuy's global website is JINGDONG E-COMMERCE (TRADE) Hong Kong CORPORATION LIMITED which is registered in Hong Kong.[28] It does not state where the personal data concerning the EU data subjects are stored, but it does say that a European user's data may be transferred to other countries and regions including Mainland China and Hong Kong.[29]

III. Transborder Data Flows in Different Scenarios Within the Framework of China-EU Cross-border E-Commerce

In the course of China-EU cross-border E-Commerce, it is inevitable that personal data of the EU data subjects will be sent across the EU border to China. Following different models of cross-border E-Commerce, in each model there are different scenarios of transborder data taking place.

1. Data flows from an EU controller to a Chinese controller or processor

The first and least controversial scenario is that an EU-based controller transfers personal data to a Chinese controller or processor. This happens, for example, when E-Commerce platforms established in the EU (such as Amazon, Wish) send personal data

[25] AliExpress.com Privacy Policy, available at https://helppage.aliexpress.com/buyercenter/questionAnswer.htm?spm=a2g0o.home.0.0.650c21450ipUX0&isRouter=0&viewKey=1&id=1000099018&categoryIds=9205401, last visited on 18.05.2020.
[26] Ibid. Section J.
[27] Joybuy Privacy Policy, version 25.05.2018, available at https://help.joybuy.com/help/question-535.html, last visited on 18.05.2020.
[28] Ibid.
[29] Ibid.

from the EU to Chinese sellers or logistic service providers. Under such circumstances, personal data are collected by the EU based platform first, and then transferred to a controller or processor that is established in a third country.

2. Data flows from the EU to China without an EU established controller

Another scenario of the transborder data flow is that personal data of the EU data subjects are sent across the EU border to China, without the involvement of a data controller established in the EU. This scenario of cross-border data flow can appear in several cross-border E-Commerce models.

2.1 Personal data directly transferred by an EU data subject to a Chinese data controller

As analyzed above, by means of providing products or services per own websites or apps, some Chinese product or service providers collect personal data of EU data subjects directly per these websites or apps. The data controller, namely the party that determines the purposes and means of the processing of personal data, is the provider that is located in China. For example, in the above-mentioned OnePlus case, the data controller is OnePlus Technology (Shenzhen) Co., Ltd. that locates in Shenzhen, China. Further, it is rather usual that the server and data center for the website or app is also located outside of the EU, where the data controller resides. When EU users visit the website or app, their personal data are collected by the data controller using technologies such as cookies, or when users input personal data to register or buy products on the website or app, these personal data are directly sent to the server that is located outside of the EU. Thus, personal data of EU data subjects flows across the EU border to China in the above-described circumstances, but without a data controller established in the EU as a transferor. The transborder data flow happens directly between the concerned data subject and the data controller located in China. The same could also apply to cross-border E-Commerce platforms. If the data controller and the

server locates in Mainland China or in Hong Kong,[30] the personal data are also sent directly by EU users to the data controller located in China.

2.2 Personal data transferred from an EU processor to a Chinese controller

Against the background of intensified restrictions on transborder data transfer worldwide, cross-border businesses relying on cross-border data flows are more and more under pressure to store personal data within the jurisdiction where the personal data is collected, partly as a response to the uncertainties associated with the transborder data transfer.[31] Moreover, using a local server to support the technical operation of the E-Commerce platform, would potentially promote the website visit experience. Thus, some cross-border E-Commerce platforms engage a data processor within the EU to store the data locally. Taking AliExpress as an example, AliExpress designates Singapore E-Commerce Private Limited established in Singapore as the data controller for the processing of personal data concerning EU data subjects.[32] However, for the data subjects within the EU, their personal data will be stored in Germany.[33] In this stage, personal data of the EU data subjects are kept within the EU.

However, since these E-Commerce platforms belong to Chinese giant E-Commerce groups with their headquarters in Mainland China, personal data might be transferred to Mainland China for (further) processing. As a matter of fact, the privacy policies of AliExpress have noted that personal data of the EU data subjects might be transferred out of the EU to third countries such as China. In such cases, transborder data flow happens in the form of the processor engaged within the EU transferring the personal data across the EU border to the non-EU data controller.

In addition, the vast majority of sellers providing products on these platforms and other

---

[30] For example, the data controller for the data processing arising from the use of Chinese E-Commerce platform Lightinthebox, is located in Hong Kong, see Privacy Note of Lightinthebox, available at https://www.lightinthebox.com/r/privacy.html?prm=1.0.87, last visited on 01.06.2020.
[31] CHANDER, Anupam, Is Data Localization a Solution for Schrems II? Journal of International Economic Law, 2020, No. 3, pp. 771-784.
[32] AliExpress.com Privacy Policy, version 26.12.2019, available at https://helppage.aliexpress.com/buyercenter/questionAnswer.htm?spm=a2g0o.home.0.0.650c21450ipUX0&isRouter=0&viewKey=1&id=1000099018&categoryIds=9205401, last visited on 20.06.2020.
[33] Ibid.

service providers are also located in Mainland China, thus, personal data concerning the EU data subjects might also be transferred to them. In such cases, transborder data transfer takes places in the form of the processor in the EU transferring the data to the non-EU sellers or other service providers under the instruction of the non-EU data controller.

Chapter 2 Extraterritorial Application of the GDPR and its Problems

No data protection law in any country or region has the same influence on the rest of the world as the European data protection law. According to the data protection law specialist Prof. Graham Greenleaf, who conducted a research and comparison of data privacy laws of 120 countries, the "European standards" of data protection had and still has far more influence outside of Europe than we thought.[34]

Prior to the current GDPR, the most influential European data protection law was the "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" ("Data Protection Directive") which came into force in 1995. In the following sections, the territorial scope in these two legislations will be analyzed. Since the Data Protection Directive was already repealed by the GDPR, emphasis will be put on the GDPR. Nevertheless, the interpretation and case law under the Data Protection Directive still plays an important role and should serve as major supporting material for the understanding and interpretation of the GDPR. Since the latter only came into force in May 2018, thus there are few official interpretation and cases under the GDPR.

Both, the Data Protection Directive (Art. 4) and the GDPR (Art. 3), stipulate the territorial scope explicitly. Compared to Art. 4 of the Data Protection Directive, Art. 3 GDPR does include new elements, but it has also inherited principles and arrangements from the Data Protection Directive. Despite the fact that a lot of attention has already been put on the territorial scope, it remains unclear, in particular for foreign companies, to determine whether and to what extent a certain foreign company's data processing activities fall within the application scope. Numerous cases illustrate that the application scope of the Data Protection Directive and the GDPR is disputed. That the territorial scope of the Data Protection Directive and the GDPR is important and yet

[34] GREENLEAF, Graham, The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108. International Data Privacy Law 2012, Vol. 2, No. 2, pp. 68-92.

ambiguous, is also verified by the fact that the Art. 29 Working Party, an advisory body made up from the data protection authorities of the Member States under the Data Protection Directive, has issued opinions on the applicable law matter twice.[35] The European Data Protection Board ("EDPB"), the body under the GDPR undertaking the function of the Art. 29 Working Party, has also drafted a guideline on the same matter shortly after its establishment[36]. This is partly because some of the key notions in the provision regulating the territorial scope are impossible to define in a few words. As Dan Jerker B Svantesson puts it, it is "the legislator's dream and the judge's nightmare"[37].

Thus, this chapter will first make an in-depth analysis of Art. 3 GDPR (territorial scope), focusing on the opinions of the Art. 29 Working Party and the guidelines of the EDPB, as well as the case law of the CJEU. Based on this *de lege lata* analysis, a judgement will be made regarding what kind of data processing activities identified in chapter 1, carried out by the E-Commerce operators located outside of the EU, are subject to the GDPR. Subsequently, the long discussed jurisdictional controversy about the wide application scope achieved by Art. 3 will be introduced and assessed. In the end, the problems arising from the wide application scope of the GDPR per Art. 3 will be emphasized.

I. Art. 3: Territorial Scope of the GDPR

1. Controllers or processors with data processing relevant establishment in the EU

Art. 3 (1), modified based on Art. 4 (1) (a) of the Data Protection Directive, is directed at companies that have at least one data processing relevant establishment in the EU. According to Art. 3 (1), the GDPR will apply to the processing of personal data "in the

[35] Art. 29 Working Party, Opinion 8/2010 on Applicable Law, adopted on 16 December 2010; Art. 29 Working Party, Update of Opinion 8/2010 on Applicable Law in Light of the CJEU Judgement in Google Spain, 16 December 2015.
[36] EDPB, Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3), version 2.1, 07 January 2020.
[37] SVANTESSON, Dan Jerker B., Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation. International Data Privacy Law, 2015, Vol. 5, pp. 226-234.

context of the activities of an establishment of a controller or a processor in the Union".[38] What differs it from Art. 4 (1) (a) of the Data Protection Directive is that, under Art. 3 (1) GDPR, both the data processing relevant establishment of the controller and that of the processor are able to trigger the application of the GDPR to the controller or the processor. For the rest, Art. 3 (1) confirms the opinions of the Art. 29 Working Party and the court practices of the CJEU without many substantial changes.

1.1 Establishment

The Art. 29 Working Party began to deal with the interpretation of "establishment" as early as 2010 in its Opinion 8/2010 on Applicable Law.[39] This Opinion invoked recital 19 of the Data Protection Directive and addressed that, an establishment must have two elements: stable arrangement, real and effective activities through this stable arrangement.[40] This is further confirmed by the EDPB in its Guidelines regarding the territorial scope of the GDPR (Art. 3).[41]

1.1.1 Stable arrangement

The Art. 29 Working Party referred to the cases of the CJEU regarding to the "stable arrangement" under the TFEU. The CJEU required, in these cases, that for a stable arrangement to exist, it must be provided that "human and technical resources necessary for the provision of particular services are permanently available".[42] However, the Art. 29 Working Party also noted that it is unclear whether and to what extent the CJEU will consistently follow its interpretation of the "stable arrangement" under the TFEU in data protection law cases. After all, the goal and objective of these two legal fields are quite different. Under the data protection law, the CJEU has expressly noted that the concept of establishment should be flexible without being formally defined.[43] The

[38] Art. 3 (1) GDPR.
[39] Art. 29 Working Party, Opinion 8/2010 on Applicable Law, 16 December 2010, p.11.
[40] Ibid.
[41] EDPB, Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3), version 2.1, 07 January 2020.
[42] Ibid.
[43] CJEU, C-230/14,01.10.2015, para. 29.

CJEU further stated that in some occasions, a single representative could constitute a stable arrangement if, according to the specific circumstances, it shows a sufficient degree of stability through necessary equipment for the involved activities.[44] This interpretation of the CJEU seems to emphasize that a stable arrangement has two components, namely a human component and an equipment component. Thus, if there is only an employee in the EU, and the employee has no fixed address, no office and no other equipment in the EU, it could hardly be justified that such arrangement is "stable". It can be further observed from the CJEU's ruling in the *Weltimmo* case that a premise is not necessary for the existence of a stable arrangement. If the data controller has an office or factory with persons working there in the EU, there is no doubt that a stable arrangement exists.[45] However, if there is only an employee with equipment other than a premise in the EU, with which the activities pursued by the employee can be effectively carried out, such as a private address, a bank account or a letter box in the EU, it may well be considered a stable arrangement. Conversely, if there is only equipment but without any human activities within the EU, such as a rented server with remote access or a mere letter box, there is no stable arrangement either. Overall, for a stable arrangement to exist, a human and an equipment element as well as a sufficient degree of stability must exist.

1.1.2 Real and effective activities

Further, with regard to the "real and effective activities", both the Art. 29 Working Party and the EDPB confirmed the CJEU's ruling in the *Weltimmo* case that the existence of any minimal activity is sufficient.[46] These activities include for example, contacting customers, dealing with complaints, conducting bank transactions, putting on advertisement etc. The real and effective activities pursued by the local establishment does not need to have any connection to the data processing itself in this stage, as this will be further examined in the next step as regard to whether the data processing is

[44] Ibid.
[45] See also BORGES, Georg, Kapitel 3, in: HELFRICH, Marcus; FORGÓ, Nikolaus; SCHNEIDER, Jochen, Operational Data Protection (Betrieblicher Datenschutz). C.H.BECK, p. 50.
[46] Art. 29 Working Party, Update of Opinion 8/2010 on Applicable Law in Light of the CJEU Judgement in Google Spain, 16 December 2015, p. 11, and EDPB, Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3), 07 January 2020, version 2.1, p. 8.

carried out in the context of the activities of the local establishment.[47]

In this sense, the opinions of the Art. 29 Working Party and the guideline of the EDPB did provide some clearness in determining the existence of an establishment in the EU, however, the whole framework of application conditions seem still relatively vague, since the aforementioned decisive factors are abstract and mostly a matter of degree (for example, the degree of stability and the degree of effectiveness), whether these factors exist in an individual case must be interpreted "in the light of the specific nature of the specific nature of the economic activities and the provision of services concerned"[48]. Thus, how the ECJU examine these factors in relevant cases could probably provide important clarifications.

The Weltimmo case

A landmark case for the interpretation of the "establishment" is the *Weltimmo* case.[49] In this case, the in Slovak registered company *Weltimmo* runs a website dealing property located in Hungary. It also has a representative in Hungary with Hungary address, a bank account for the recovery of debts and a letter box for the management of business affairs. The question arises as, whether these human and facility resources of *Weltimmo* in Hungary together constitute an establishment in Hungary. In the judgement, the CJEU first recalled the elements necessary for such an establishment, namely a stable arrangement and the effective and real exercise of activities through this arrangement. A stable arrangement further requires a sufficient degree of stability and necessary human and technical resources. Obviously, the court held the opinion that the one representative together with the bank account and letter box of *Weltimmo* in Hungary provides for enough human and equipment resource for the company's property business in Hungary. Though the Court did not mention which fact is decisive for the stability test, it is reasonable to assume that the existence of an address of the representative in Hungary (registered in the Slovak company register) must have played a role here. Furthermore, in determining whether real and effective activities are pursued in Hungary, the Court argued that, since *Weltimmo* runs property dealing

[47] KLAR, Manuel, Art. 3, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H.BECK, 2nd edition 2020, p.51.
[48] CJEU, C-230/14, 01.10.2015, para. 29.
[49] CJEU, C-230/14, 01.10.2015.

websites concerning properties located in Hungary, using Hungarian and charge an advertisement fee, it is obvious that *Weltimmo* pursues a real and effective activity in Hungary.[50] Therefore, the court came to the conclusion that this information (of what *Weltimmo* has in Hungary) is "capable of establishing the existence of an 'establishment'".

The *Weltimmo* case is enlightening in the sense that it made clear the minimal human and technical resource -in the presented case one representative with a bank account and letter box- can be interpreted to have fulfilled the stable arrangement element. The existence of a premise in the sense of a fixed space, which from a traditional perspective seems to be necessary for an establishment, is abandoned in this case. In addition, the other element, namely the exercise of real and effective activity, can also be met with minimal activities. By reducing most requirements to a minimal level, the notion establishment is broadly interpreted.

1.2 Processing carried out in the context of the activities of the establishment

If an establishment does exist, it is further to determine whether the processing of personal data is carried out in the context of the activities of this establishment. This means, even if there is an establishment within the EU, it does not automatically lead to the data controller or processor subject to the GDPR per Art. 3 (1). Furthermore, the activities of this local establishment must have a sufficient connection to the data processing.

Likewise, in order to decide whether the processing of personal data is carried out in the context of the activities of this establishment, a case-by-case review would be necessary. In the famous Google Spain case,[51] the CJEU has established that the activities of the local establishment must be "inextricably linked" to the data processing, meanwhile, the local establishment does not necessarily have to take any direct part in the data processing itself.[52] In the same case, the CJEU further recognized that an

[50] CJEU, C-230/14, 01.10.2015, para. 32.
[51] CJEU, C‑131/12, 13.05.2014.
[52] CJEU, C‑131/12, 13.05.2014, para. 52 and 56.

economical link between the activities of the local establishment and the data processing of the data controller outside of the EU could constitute an inextricable link.[53] In this respect, the Art. 29 Working Party and the EDPB further confirmed that the raising of revenue by a local establishment in the EU to the extent that such activities can be considered as inextricably linked to the processing of personal data may bring the data processing by a non-EU controller or processor under the GDPR.[54]

It must be noted that the CJEU's ruling in the Google Spain case only refers to the activities of search engine and its advertisement, in other business models there might be different factors or different forms of "inextricable link" to consider. The Art. 29 Working Party has concluded that, in terms of the reference value of the case, the judgement not only applies to business models that offer free services in the EU and are financed by making use of the user data, but also to models such as offering services in the EU in return for membership fees or subscriptions.[55] Ultimately, again, the facts in the specific case are decisive. In general, except for the economic link as showed in the Google Spain case, other connections between the activities of the local establishment and the data processing, such as the local establishment has a direct impact on the data processing or is technically instead of economically linked to the data processing, could also be considered an inextricable link. As the CJEU emphasized, to ensure a comprehensive protection to the fundamental rights and freedoms of natural persons, the application scope of the GDPR cannot be interpreted restrictively.[56]

Notably, Art. 3 (1) is not only of importance for data controllers located in the EU, but even more crucial for data controllers that are located outside of the EU but have establishment in the EU, since this might bring the relevant data processing outside of the EU under the application of the GDPR. In the event that the data controller outside of the EU has several establishments in the EU, the Art. 29 Working Party noted in its Opinion that for every establishment, it needs to be assessed whether there are data processing activities carried out in the context of that establishment.[57] If so, the

---

[53] CJEU, C‑131/12, 13,05,2014, para. 56.

[54] Art. 29 Working Party, Update of Opinion 8/2010 on Applicable Law in Light of the CJEU Judgement in Google Spain, adopted on 16 December 2015, p. 4-5; EDPB, Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3), version 2.1, 12 November 2019, p. 8.

[55] Art. 29 Working Party, Update of Opinion 8/2010 on Applicable Law in Light of the CJEU Judgement in Google Spain, adopted on 16 December 2015, p. 5.

[56] CJEU, C‑131/12, 13.05.2014, para. 52.

[57] Art. 29 Working Party, Update of Opinion 8/2010 on Applicable Law in Light of the CJEU Judgement in Google

respective data processing activities have to comply with the data protection law of the Member State where the establishment locates.

1.3 Practical significance for cross-border E-Commerce operators

As showed in the introduction of this dissertation, many Chinese E-Commerce platforms have local branches in the EU, for example, Alibaba Group who owns AliExpress has several offices and shops in Europe. The Privacy Policy of Alibaba shows that the data controller for the processing of personal data of EU data subjects is Alibaba.com Singapore E-Commerce Private Limited,[58] a company registered in Singapore, thus, the data controller is not located in the EU. It is not revealed where the personal data concerning to EU data subjects is processed, whether inside or outside of the EU. According to Art. 3 (1) GDPR, it primarily needs to be determined whether the local branches of Alibaba group in the EU could be evaluated as establishments within the meaning of Art. 3 (1). If these local branches have a stable structure consisting of sufficient human and equipment resources, which carry out real and effective activities, such as selling, contacting, assisting or advertising, even if they are minimum in scope and intension, these local branches will be assessed as establishments within the meaning of Art. 3 (1).

In next step, it must also be examined what data processing operations are carried out in the context of which establishment. As noted above, not all establishment is a data processing relevant establishment. The activities of the local establishment must be inextricably linked to the data processing. Under the framework of cross-border E-Commerce discussed in this dissertation, personal data concerning to the EU data subjects is mostly either collected by using tracking techniques such as cookies or other social Plugins, when the data subjects visit the E-Commerce website to review or buy products or services, or it is input by the data subjects when they register with the website or order a product or service. Against this backdrop, the local branches in the EU that carry out sales-related activities, including market research or logistic or

Spain, 16 December 2015, p. 6.

[58] AliExpress.com Privacy Policy, Art. J. Visitors from the European Union, available at https://service.aliexpress.com/page/knowledge?pageId=37&category=1000022028&knowledge=1060015216&language=en, last visited on 20.06.2020.

technical support for the provision of products or services, should be considered to be inextricably linked to the above identified data processing.[59] As a consequence, the GDPR or more specifically, the data protection law of the Member State where that sales office locates will apply to the relevant data processing activities that are carried out in the context of that sales office. Meanwhile, in so far as Alibaba also has a cloud center in Frankfurt, Germany, which provides cloud services for business customers through its own website and sales network, the cloud center could hardly be considered inextricably linked to the data processing with regard to the E-Commerce website, unless the data collected through the use of the E-Commerce website are stored there.

To sum up, operators of cross-border E-Commerce websites or apps that collect personal data in the EU may be subject to the GDPR per Art. 3 (1), even if the data controller itself is not located in the EU, nor does the data processing take place in the EU.

2. Controllers or processors without data processing relevant establishment in the EU

Compared to Art. 3 (1), Art. 3 (2) is directed at data controllers or processors that are located outside of the EU and have no data processing relevant establishment in the EU. From a historic point of review, Art. 3 (2) establishes a new principle for the application scope of the EU data protection law: in German literature usually called the "Marktortprinzip" (Market place principle). This constitutes a fundamental change to the previous Data Protection Directive.

2.1 From making use of equipment situated on the territory of EU to the marketplace principle

Pursuant to the outdated Data Protection Directive, if the data controller has no data processing relevant establishment in the EU, the Data Protection Directive could still

[59] EDPB, Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3), version 2.1, 12 November 2019, p. 8.

apply to the processing if the controller *"for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community."*[60] This reliance on the existence of an equipment on the territory of the EU was already under criticism in the era of the Data Protection Directive. It was criticized that requiring a strict connection of the data processing with the EU territory leads to the result that some internet-based data processing activities might escape the application of the EU data protection law.[61] Before the data protection reform that resulted in the promulgation of the GDPR, the CJEU has already referred to ideas of the marketplace principle to make judgements.[62]

To put it in simple terms, the marketplace principle generally means the law of the targeted market should apply to the provision of goods or services on the market.[63] Specifically under the GDPR, this means if the offering goods or services targets at data subjects in the EU, and the data processing is related to such offering goods or services on the European market, the GDPR shall find application to such data processing activities.[64] The marketplace principle is not entirely new in the EU law, as it is already widely recognized in the competition law, consumer protection law when interpreting applicable law issues related to the internet.[65] Within the EU, the introduction of the marketplace principle in the GDPR is primarily welcomed since it helps to avoid circumvention of the GDPR by data controllers or processors located outside of the EU, as well as ensures fair completion conditions for companies within and outside of the EU. However, among scholars and companies, in particular those outside of the EU, it is criticized as uncertain,[66] long-arm and overreaching[67].

---

[60] Art. 4 (1) (c) Data Protection Directive.
[61] KLAR, Manuel, Art. 3, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H.BECK, 2nd edition 2020, p. 15.
[62] For example, in the Google Spain case, see KLAR, Manuel, Art. 3, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H.BECK, 2nd edition 2020, p. 17.
[63] See KLAR, Manuel, Art. 3, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H.BECK, 2nd edition 2020, p. 9.
[64] Recital 23 and Art. 3 (2) GDPR.
[65] See SYDOW, Gernot, EU GDPR (Europäische Datenschutzgrundverordnung). Nomos, 2nd edition 2018, p. 59.
[66] SVANTESSON, Dan Jerker B, Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation. International Data Privacy Law, 2015, Vol. 5, p. 232; SCHWARTZ, Paul M, Information Privacy in the Cloud. University of Pennsylvania Law Review, 2012, Vol. 161, p. 1623.
[67] KUNER, Christopher, The European Union and the search for an international data protection framework. Groningen Journal of International Law, 2014, Vol. 2, p. 61; MOEREL, Lokke, The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide? International Data Privacy Law, 2011, Vol. 1, No. 1, p. 46.

2.2 Processing related to the offering of goods or services to data subjects in the EU

As noted above, the connecting factor of "equipment" in the previous Art. 4 (1) (c) is abandoned in the GDPR. It must be noted the application of Art. 3 (2) is limited to the processing of personal data of data subjects in the EU. The wording "in the EU" indicates that a EU nationality or residence is not necessary, it is sufficient if a data subject is temporarily present in the EU when the offering of goods and services or monitoring behaviors take place.[68] The EDPB holds that this provision of the GDPR reflects a fundamental value of the EU primary law, since the right to the protection of personal data is considered by the "Charter of Fundamental Right of the European Union" as a fundamental right for everyone.[69] By this definition, even the processing of personal data related to a tourist or passenger passing the EU territory by a controller established outside of the EU will lead to the application of the GDPR, provided the other conditions are met.

The GDPR applies when the processing activities are related to the offering of goods or services to the data subjects in the Union, irrespective of whether a payment is required. Since the controller or processor has no establishment in the EU, the main scenario under section 2 involves the internet. Due to the open nature of the internet, almost all websites are accessible from the EU, thus, merely the accessibility of a website in the EU should not trigger the application of the GDPR, otherwise all website holders will potentially have to comply with the GDPR. Therefore, both Recital 23 of the GDPR and the Guidelines 3/2018 on the territorial scope of the GDPR demonstrate that the offering of goods or services must be directed at the data subjects in the EU.[70] However, it is not necessary that the offer of goods or services only or mostly aimed at the EU market, on the contrary, if the controller makes it clear that the goods or services are to be offered to the whole world, it is obvious that the controller or processor also intend to offer goods or services in the EU.[71] Recital 23 lists some circumstances

[68] EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.1, 12 November 2019, p. 14.
[69] Ibid.
[70] Ibid.
[71] HORNUNG, Gerrit, Art. 3, in: SIMITS, S.; HORNUNG, G.; SPIECKER gen. DÖHMANN, I, Data Protection Law (Datenschutzrecht), Nomos, 1st edition 2019, p. 50.

indicating that the controller intends to offer goods or services to data subjects in the EU, it is however by no means exhaustive. Therefore, the matter is more or less an individual judgement.

2.3 Processing related to the monitoring of behavior of the EU data subjects

Alternatively, the monitoring of behavior of a data subject in the EU could also trigger the application of the GDPR, provided the behavior itself takes place in the EU. Unlike Art. 3 (2) (a) which expressly requires the data controller or processor to target at the data subject of the EU, Art. 3 (2) (b) and its recital does not specify whether an intention to target should be in place for the monitoring activities. Some scholars thus hold the opinion that Art. 3 (2) (b) goes beyond the marketplace principle due to the lack of a targeting element.[72] The justification of Art. 3 (2) (b) is also questioned, since the use of tracking technologies such as cookies is so popular that almost every website could be brought into the application scope of the GDPR, even if it does not target at EU data subjects and thus shows a rather weak link to the EU.[73]

In this regard, the EDPB noted that "monitoring" itself indicates that the controller "has a specific purpose in mind for the collection and subsequent use of the relevant data".[74] However, the fact that the controller or processor has a specific purpose for the data processing in mind is not equivalent to targeting at the EU data subjects. For example, a Chinese website uses cookies to track user activities with the purpose of analyze user behavior, however, the website is only available in Chinese and directs at Chinese users. If a European user randomly visits the website in the EU, by so doing his personal data is collected by the Chinese website operator, according to the current Art. 3 (2) (b), the Chinese website operator has to comply with the GDPR with regard to this specific purpose of processing personal data. This outcome seems outrageous and contradicts to the CJEU's altitude in other rulings that the mere accessibility of the website in the EU

[72] SPINDLER, Gerald, Data Protection and Privacy Rights on the Internet-the Framework for Research Tasks and Need for Reform (Datenschutz- und Persönlichkeitsrechte im Internet-der Rahmen für Forschungsaufgaben und Reformbedarf), GRUR, 2013, No. 10, p. 1003; BRAUNECK, Jens, Market Place Principle of the GDPR: Global Validity for EU Data Protection (Marktortprinzip der DSGVO: Weltgeltung für EU-Datenschutz?) EuZW, 2019, No. 12, pp. 496-497.
[73] See KLAR, Manuel, The Extraterritorial Effect of the New European Data Protection Law (Die extraterritoriale Wirkung des neuen Europäischen Datenschutzrechts). Datenschutz und Datensicherheit, 2017, Vol. 41, No. 9, p. 536.
[74] EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.1, 12 November 2019, p. 20.

should not trigger the application of the EU data protection law.[75] Some scholars try to justify Art. 3 (2) (b) by arguing that, personal profiles are highly important, so that it is necessary to ensure that data controllers respect minimum data protection rules of the EU.[76] The EDPB even suggested that both for Art. 3 (2) (a) and Art. 3 (2) (b), the element of "targeting" must be in place.[77] However, the EDPB also recognized that as opposed to Art. 3 (2) (a), Art. 3 (2) (b) and its recital does not mention targeting, it remains unclear how then the EDPB came to the conclusion that the element of targeting must be in present for Art. 3 (2) (b) to apply.[78] The issue needs to be further clarified by the case law of the CJEU.

2.4 Application to cross-border E-Commerce operators

A major scenario for the application of Art. 3 (2) is internet-based activities. Nowadays, collecting personal data in relation to offering products or services, or monitoring behavior is more a normality than an exception for E-Commerce businesses. Without processing personal data, E-Commerce providers would not be able to provide products or services to their customers, without monitoring user behavior, a major trend of the E-Commerce, user customized products or services will not exist.

Under the Data Protection Directive, due to the requirement of a link to the EU territory in the then Art. 4 (1) (c), it is difficult to bring online business which has no territorial link to the EU under the regulation of the EU data protection law, without interpreting Art. 4 (1) (c) so widely that it contradicts the wording and legislative history of the Data Protection Directive.[79] This obstacle is removed by Art. 3 (2) GDPR, which introduces the targeting element as the connecting factor for the application of the EU data protection law to the data processing carried out by data controllers or processors

[75] KLAR, Manuel, The Extraterritorial Effect of the New European Data Protection Law (Die extraterritoriale Wirkung des neuen Europäischen Datenschutzrechts). Datenschutz und Datensicherheit, 2017, Vol. 41, No. 9, p. 536.
[76] DE HERT, Paul; CZERNIAWSKI, Michal, Expanding the European Data Protection Scope Beyond Territory. International Data Privacy Law, 2016, Vol. 6, No. 3, p. 240-241.
[77] EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.1, 12 November 2019, p. 15.
[78] KLAR, Manuel, Art. 3, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H.BECK, 2nd Edition 2020, p. 25.
[79] See in detail MOEREL, Lokke, The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide? International Data Privacy Law, 2011, Vol. 1, No. 1, p. 41.

located outside of the EU.

Therefore, under the GDPR, in the event that a Chinese E-Commerce operator provides products or services to EU customers, or monitor European user behaviors by using tracking techniques, the collection of personal data of the EU data subjects directly by the Chinese E-Commerce operator and the sending of such data to China as a result of the visiting of the EU data subjects of E-Commerce site will be subject to the GDPR per Art. 3 (2).

II. Jurisdictional Controversy Regarding the Territorial Scope of the GDPR per Art. 3

The broad scope and aforementioned uncertainty of Art. 3 has led to severe concerns in non-EU countries. Commenters and law practitioners frequently talk about the extraterritoriality of the GDPR.[80] It is no doubt that the GDPR applies to controllers and processors located outside of the EU and personal data processing activities taking place outside of the EU. The adoption of Art. 3 (2), removing the "equipment" requirement, further weakens the territorial link of the data processing activities of the controllers or processors and the EU territory.

That the GDPR has extraterritorial character is claimed by a lot of data protection law scholars and commenters.[81] However, the concept of extraterritoriality is one that full of confusion and mixture of other unclarified concepts. Though it is frequently discussed in the literature,[82] due to its complexity, the following part will give a brief introduction to the meaning and context of this concept.

[80] See for example AHMAD, Imran, Extraterritorial Scope of GDPR: do Canadian businesses Need to Comply?, available at https://www.millerthomson.com/en/blog/mt-cybersecurity-blog/extraterritorial-scope-gdpr-canadian-businesses-need-comply/. Last visited on 01.06.2020.
[81] Ibid.
[82] For example, SVANTESSON, Dan Jerker B, Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation. International Data Privacy Law, 2015, Vol. 5; KUNER, Christopher, Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law. International Data Privacy Law, 2015, Vol.5p. 235-245.

1. Extraterritoriality under public international law

In order to explore the extraterritoriality of the EU data protection law, an introduction or clarification to the concept "extraterritoriality" is inevitable. According to the Oxford English Dictionary, extraterritoriality is originally referred to the privilege of ambassadors of "being regarded as outside the territory of the power to which they are sent, and therefore of being free from its jurisdiction". Later on, this term has been extended to imply "the right of jurisdiction of a country over its nationals abroad, or the status of persons living in a foreign country but not subject to its laws".[83] Beyond that, a legal definition is not found under any written law. Extraterritoriality has rather gained its significance in the academia. Having reviewed the various academic publication, it becomes obvious that the term "extraterritoriality" or "extraterritorial" is used in a much broader way in the legal field than its denotation stated in the Oxford English Dictionary. In particular, jurisdiction claims of a sovereign state towards other nationals outside its territory are also perceived as extraterritorial claims. As a matter of fact, this kind of jurisdiction claims is perhaps much more extraterritorial than the jurisdiction claims over its own nationals abroad. Thus, the term "extraterritoriality" is far away from a self-evident concept, neither in international law nor in other fields of law. Since conflict matters beyond one's own territorial often land in international public law and this dissertation focus mainly on the extraterritoriality of the European data protection law, below I will focus on the term extraterritoriality in public international law and data protection law.

Since "extraterritorial" is usually, also in the context in this dissertation, used to describe the scope of a sovereign state's jurisdiction, it is necessary to clarify what kinds of jurisdiction we are talking about.

1.1 Jurisdiction

However, jurisdiction itself is not a concept that can be defined in a clear and concise sentence either. Prof. Mann wrote in 1964, "Jurisdiction involves a state's right to

[83] https://www.oed.com/view/Entry/67138?redirectedFrom=extraterritoriality#eid, last visited on 15.06.2020.

exercise certain of its powers".[84] In this sense, although different meanings the term jurisdiction may have in different contexts, jurisdiction mostly has a connection with a sovereign state exercising its legal power. Since public international law regulates the relationships between states, if the assertion of jurisdiction by a state only involves domestic concerns, such jurisdiction will not come under the sight of the public international law. Thus, Jurisdiction in public international law concerns two elements: a sovereign state's right to exercise jurisdiction over a specific subject matter and the same kind of right, stronger or weaker as they may be, of other states. In other words, public international law ensures that one sovereign state's assertion of jurisdiction does not improperly intervene the sovereignty of other states.[85]

Compared with the rather unambiguous definition of jurisdiction, the types of jurisdictions have gained significantly more consensus under the international law. Traditionally, jurisdiction can be divided into three types:[86]

a) Prescriptive or legislative jurisdiction, i.e., the power to make law or make its law applicable to a certain subject matter;

b) Adjudicative or judicial jurisdiction, i.e., the power to adjudicate a certain subject matter, in most cases through the court;

c) Enforcement jurisdiction, i.e., the power to enforce the law.

Some scholars also try to introduce one more type of jurisdiction to the current categories, that is, the investigative power, which Dan Jerker B described as the power to investigate a matter.[87] Since in most cases, investigation is a necessary precondition for deploying enforcement measures, in this dissertation, the author will use enforcement jurisdiction in the sense that it also encompasses investigation jurisdiction.

Since this part focuses on the extraterritoriality of the GDPR and its application to Chinese data controllers or processors, emphasis will be put on the prescriptive and

---

[84] MANN, Friedrich Alexander, The Doctrine of Jurisdiction in International Law (Volume 111). Collected Courses of the Hague Academy of International Law. Available at: http://dx.doi.org/10.1163/1875-8096_pplrdc_ej.9789028614826.001_162.2, last visited on 16.06.2020.
[85] RYNGAERT, Cedric. Jurisdiction in International Law. OUP Oxford, 2015, p.6.
[86] Ibid. p. 50-76.
[87] SVANTESSON, Dan Jerker B, The Extraterritoriality of EU Data Privacy Law - its Theoretical Justification and Its Practical Effect on US Businesses. Stanford Journal of International Law, 2014, Vol. 50, p.53.

enforcement jurisdiction, that is, the extraterritorial feature of the GDPR itself and its enforcement, in particular in China.

1.2 Extraterritorial jurisdiction

1.2.1 Definition

As mentioned above, extraterritoriality or extraterritorial jurisdiction is not an uncontroversial concept in the context of international law. A universally accepted definition does not exist.

Among the various interpretations of this term, the International Law Commission of the United Nations interprets extraterritorial jurisdiction as "an attempt to regulate by means of national legislation, adjudication or enforcement the conduct of persons, property or acts beyond its borders which affect the interests of the state in the absence of such regulation under international law".[88] In the light of the aforementioned jurisdiction concept, this dissertation intends to use this interpretation of the International Law Commission since it is the most official interpretation and also employed by some active and prestigious scholars in their relevant articles regarding extraterritorial jurisdiction.[89]

1.2.2 Basis for extraterritorial jurisdiction under public international law

The attitude of the public international law towards extraterritorial jurisdiction is rather ambiguous. In the famous Lotus case, the Permanent Court of International Justice established the "prohibitive rule" for the exercise of extraterritorial prescriptive and adjudicative jurisdiction, meaning states are in principle free to claim extraterritorial prescriptive and adjudicative jurisdiction, unless there is a prohibitive rule in public international law forbidding them to do so.[90] In regard to enforcement jurisdiction, states are forbidden to exercise extraterritorial enforcement jurisdiction unless a

[88] International Law Commission, Report on the Work of the Fifty-eighth Session (2006), Available at http://legal.un.org/ilc/reports/2006/. Last visited on 24.02.2019.
[89] For example, KUNER, Christopher, Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law. International Data Privacy Law, 2015, Vol.5, pp. 235-245.
[90] KAMMINGA, Menno, Extraterritoriality. Max Planck Encyclopedias of International Law, 2012, p. 1070-1077.

permissive rule exists.[91]

1.2.2.1 Prescriptive and adjudicative Jurisdiction

With regard to prescriptive and adjudicative jurisdiction, this "prohibitive rule" has encountered tons of criticism since it only aggravates the conflicts caused by different states claiming jurisdiction over the same subject. Contrary to the Lotus case, customary international law which is based on states practice represents the view that extraterritorial prescriptive and adjudicative jurisdiction should be prohibited unless there is a permissive rule in international law.[92]

a. Type of prescriptive and adjudicative jurisdiction principles

The basic as well as most widely accepted principles for prescriptive and adjudicative jurisdiction in customary international law was laid down by the 1935 Harvard Research Draft Convention on Jurisdiction with Respect to Crime ("Harvard Draft"). The Harvard Draft generally requires a genuine link between the state which claims jurisdiction and the subject matter.[93] Such link does not have to be a territorial one, it may also be any other "genuine link", for instance to protect a state's own nationals or public interests.[94] Based on the different links, the Harvard Draft described five types of jurisdiction grounds, on which jurisdiction was claimed by states at that time:

1. Territoriality principle, determining jurisdiction based on the place where the offense is committed (a territorial link), which is also called the subjective territoriality principle. The subjective territoriality principle should be distinguished from the objective territoriality principle. Pursuant to the objective territoriality principle, a state gains jurisdiction if a "constitutive element" of the to be regulated

[91] Ibid.
[92] RYNGAERT, Cedric, Jurisdiction in International Law. Oxford University Press, Oxford, 2015.
[93] Ibid, p.34.
[94] Ibid.

conduct occurred on the territory of the State.[95]

2. Nationality principle, determining jurisdiction based on the nationality of the offender;

3. Passive personality principle, determining jurisdiction based on the nationality of the offended;

4. Protective principle, determining jurisdiction based on the harm to the state;

5. Universal principle, determining jurisdiction based on the custody of the offender.

Despite the fact that the Harvard Draft originally aimed at criminal cases and was published almost a century ago, there are no jurisdiction grounds accepted more broadly in today's public international law. It is however worthy noting that the "effects doctrine" gains more and more acceptance especially in the economic law. Pursuant to the effects doctrine, a state may exercise jurisdiction if an alien conducts an offense which is beyond its territory but has substantial effects within its territory.[96] The effects doctrine is regarded as an extension of the objective territoriality principle and differentiates from the latter in that it does not require the conduct at least partially take place in the territory of the state claiming jurisdiction over the conduct.[97]

An examination of the above-mentioned principles reveals that most of these principles are actually extraterritorial since they are not based on the territory where the offense was committed, excluding the subjective territoriality principle. Yet these principles are the most frequently used ones to justify a sovereign State's jurisdiction claims. Only the acceptance of each principle by the states varies from sector to sector.

b. Acceptance of prescriptive and adjudicative jurisdiction principles

It is commonly recognized that the territoriality principle (to be exact, the subjective territoriality principle) is the primary jurisdiction principle in the public international

[95] International Law Commission, Report on the Work of the Fifty-eighth Session (2006), Available at http://legal.un.org/ilc/reports/2006/. Last visited on 15.07.2020.
[96] Ibid.
[97] Ibid.

law and also the least controversial one. However, this assertion could probably only be proven true with regard to the subjective territoriality principle. It is thus necessary to make a distinguish between the subjective territoriality principle and the objective territoriality principle. The subjective territoriality principle as a jurisdiction basis has gained consensus traditionally and universally,[98] which is considered by the Harvard Draft to be accepted "everywhere regarded as of primary importance and of fundamental character".[99] On the contrary, relying on the objective territoriality principle is not in all cases unambiguous.[100] The application of the objective territoriality principle inherently presupposes that the conduct relates to more than one country. This inevitably leads to the question as to whether the state where a constitutive element of the conduct takes place or the state where the conduct was committed is more entitled to claim jurisdiction over the subject matter. Therefore, although the objective territoriality principle still falls within the catalogue of territoriality principle, it actually contains some sort of extraterritorial elements. Indeed, the United Nations Report of the International Law Commission considered the objective territoriality principle to be one of the jurisdiction principles justifying extraterritorial jurisdiction claims.[101]

The effects doctrine is deemed an extension of the objective territoriality principle. The argument is that the impact or "effect" of a conduct is also a constitutive element of that conduct.[102] With the objective territoriality principle itself being controversial and contested in whether it is in all aspects territorial, attaching a "territorial" label to the effects doctrine appears highly problematic. Though confirmed by the famous Lotus case, there is criticism with regard to what constitutes a "constitutive element" and what degree of "effects" is sufficient to justify a jurisdiction claim based thereon.[103] Lacking a commonly recognized standard, a random effect-based jurisdiction claim shows a very weak link between the claiming state and the conduct. In fact, though

---

[98] International Law Commission, Report on the Work of the Fifty-eighth Session (2006), Available at http://legal.un.org/ilc/reports/2006/. Last visited on 15.07.2020.
[99] Introductory Comment to the Draft Convention on Jurisdiction with Respect to Crime. American Journal of International Law, 1935, Vol. 29, p. 442.
[100] SVANTESSON, Dan Jerker B, The Extraterritoriality of EU Data Privacy Law - its Theoretical Justification and Its Practical Effect on US Businesses. Stanford Journal of International Law, 2014, Vol. 50, p. 53.
[101] International Law Commission, Report on the Work of the Fifty-eighth Session (2006), Available at http://legal.un.org/ilc/reports/2006/. Last visited on 15.07.2020.
[102] SAMIE, Najeeb, The Doctrine of" Effects" and the Extraterritorial Application of Antitrust Laws. Lawyer of the Americas, 1982, Vol. 14, No. 1, p. 23-59.
[103] Ibid.

originating from the objective territoriality principle, it is generally recognized that the effects doctrine is based on the "effects" instead of the "territory", thus being extraterritorial.[104]

The other extraterritorial jurisdiction principles are all more or less controversial at least in certain legal fields. According to the Introductory Comment to the Harvard Draft, the nationality principle is universally accepted, and the protective principle is claimed by most states as an auxiliary basis, the passive personality principle is claimed by some states and contested by others, the universal principle is probably the most controversial principle claimed by some states in certain legal areas but by no means universally accepted.[105]

To sum up, extraterritorial jurisdiction claims are not a rare phenomenon under the public international law for legislative and adjudicative jurisdiction. Extraterritorial claims can find its basis in the various permissive jurisdiction principles under the public international law. The word "extraterritoriality" only suggests that the jurisdiction is based on other links other than a territorial one, which may from case to case be controversial but *per se* not prohibited by the public international law, as demonstrated above. In fact, most of the states have claimed extraterritorial jurisdiction at least in certain legal areas.

1.2.2.2 Enforcement Jurisdiction

Enforcement jurisdiction refers to the power of a state to enforce its own law, either through authority orders or court judgements. Further, according to the definition engaged in this dissertation, enforcement jurisdiction also encompasses the investigation engaged by authorities such as police or courts during such law enforcement.

In contrast to prescriptive and adjudicative jurisdiction, it is well established that

[104] International Law Commission, Report on the Work of the Fifty-eighth Session (2006), Available at http://legal.un.org/ilc/reports/2006/. Last visited on 20.07.2020.
[105] Introductory Comment to the Draft Convention on Jurisdiction with Respect to Crime. American Journal of International Law, 1935, Vol. 29, p. 445.

enforcement jurisdiction is to a great extent territorial.[106] Not only was this confirmed by the judgement of the Lotus Case, it has also become a general recognized principle in the public international law theory.[107] According to this principle, on one side, a state may only take law enforcement measures within its own territory.[108] On the other side, a state is not allowed to pursue law enforcement activities on the territory of other states without the consent of the latter, whether directly or indirectly, because it will violate the other states' sovereignty.[109]

1.2.2.3 The dilemma between prescriptive, adjudicative jurisdiction and enforcement jurisdiction

As noted previously, customary international law provides at least five different jurisdiction principles, upon which states could rely to exercise prescriptive and adjudicative jurisdiction. These encompass both territorial ones as well as extraterritorial ones. Accordingly, a state may enact laws and regulations to regulate conducts of foreign citizens that take place abroad, if it holds the view that there are domestic interests connected to such conducts, invoking the passive nationality principle, the protective principle or the effects doctrine described above.

However, it is also uncontroversial that a state could only exercise enforcement jurisdiction on its own territory. This leads to a dilemma, namely a state may legislate extraterritorially, but lack the ability to enforce its law abroad. This is particularly true, when a state tries to regulate conducts of foreign subjects who have neither organizational nor financial assets in the regulating state.

Unsurprisingly, states may have various reasons to decline the enforcement of a foreign law on their own territory, since no international law obligates them to do so.[110] Thus,

---

[106] KAMMINGA, Menno, Extraterritoriality. Max Planck Encyclopedias of International Law, 2012, p. 1070-1077.
[107] CRAWFORD, James. Brownlie's Principles of Public International Law. Oxford University Press, Oxford, 2019, p. 462.
[108] MILLS Alex, Rethinking Jurisdiction in International Law. British Yearbook of International Law, 2014, Vol. 84, p. 187-239.
[109] CRAWFORD, James, Brownlie's Principles of Public International Law. Oxford University Press, Oxford, 2019, p. 462.
[110] MICHAELS, Ralf, Recognition and Enforcement of Foreign Judgements. Max Planck Encyclopedias of International Law. Available at https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-

it is largely dependent on the state in which the enforcement of a foreign law is sought, whether extraterritorial enforcement can be exercised. This could, again, vary a lot according to the nature of the enforcement as in whether it is an enforcement of public law or private law. More precisely, an administrative order or judgement issued due to the violation of a public law obligation is unlikely to be enforced in a third country, due to the generally recognized "public law taboo".[111] In contrast, a civil law judgement, for instance one concerning contract breach, is much more likely to be enforced in a third country.[112]

2. Extraterritoriality of the GDPR

Based on the definition of extraterritorial jurisdiction adopted in this dissertation, extraterritorial jurisdiction in data protection law could be defined as the attempt to regulate by means of national legislation, adjudication or enforcement the data processing activities beyond its borders which affect the interests of the state. Regarding the question, whether a certain data protection law is extraterritorial is more a fact judgement than a subjective assessment.[113] It largely depends on the applicable law rules contained in the questioned data protection law, i.e., whether the concerned data protection law applies to conducts carried out outside of the forum state's territory.

From the above analysis, it is clear that pursuant to Art.3 (1) and Art.3 (2), the GDPR applies to data processing activities carried out and controllers operating outside of the EU territory. The GDPR itself thus contains extraterritorial jurisdiction claims. From the perspective of the international public law, these extraterritorial jurisdiction claims are based on different jurisdiction principles.

Art. 3 (1) uses the connecting factor of "establishment". It seems to have based at least partly on the least controversial territoriality principle, since the controller has a physical establishment on the EU territory and the related personal data processing

9780199231690-e1848, last visited on 22.08.2020.
[111] DODGE, William S, Breaking the Public Law Taboo. Harvard International Law Journal, 2020, Vol. 43, p. 161.
[112] Ibid.
[113] SVANTESSON, Dan Jerker B, The Extraterritoriality of EU Data Privacy Law - its Theoretical Justification and Its Practical Effect on US Businesses. Stanford Journal of International Law, 2014, Vol. 50, p. 53.

activities have a close connection with the establishment. However, the GDPR applies not only to the data processing activities carried out by the local establishment, but also in the circumstance where the establishment is not directly involved in but only "inextricably linked" to the data processing activities, according to the case law of the CJEU. Such "inextricably link" also includes the economical contribution of the local establishment to the data processing activities of the controller outside of the EU. This kind of broad interpretation of the CJEU and the Art. 29 Working Party to some extent extends the territoriality principle, since there is no direct data processing taking place on the EU territory.

As for Art. 3 (2), after the removal of the element "making use of equipment situated on the EU territory" contained in Art. 4 (1) (c) Data Protection Directive, the subjective territoriality principle is entirely abandoned through Art. 3 (2) GDPR. Instead of relying on a physical connection between the data processing activities and the EU territory (the processing makes use of equipment on the EU territory), under the GDPR, the marketplace and targeting is now the trigger bringing the data processing activities outside of the EU under the regulation of the GDPR. The jurisdiction principles behind the targeting approach could be the effects doctrine or the objective territoriality principle since it focuses on the effect of the data processing activities on the individuals in the EU. This position is indeed held by a large number of scholars.[114] Further, since it is ambiguous whether Art. 3 (2) (b) requires a certain degree of targeting (the wording of Art. 3 (2) (b) rather goes against it), and it is certain that for Art. 3 (2) to apply, the data subjects must be in the EU, it could be argued that Art. 3 (2) is justified under a modified passive personality principle.[115] It is a modified passive personality principle, because the application of Art. 3 (2) does not presuppose that the data subject is a EU citizen, as opposed to the strict meaning of the passive personality principle. However, it must be considered that data subjects in the EU are mostly citizens of the EU or

[114] For example, SVANTESSON, Dan Jerker B, Extraterritoriality in Data Privacy Law. Ex Tuto Publishing, Denmark, 2013. p. 84; VERMEULEN, Gert; LIEVENS, Eva (Hg.), Reconciling the (Extra)territorial Reach of the GDPR with Public International Law. Data Protection and Privacy Under Pressure, Transatlantic Tensions, EU Surveillance and Big Data, 2017, p. 96; TAYLOR, M. S. C., et al, Permissions and prohibitions in data protection jurisdiction. Brussels privacy hub working paper 2016, Vol. 2, p. 17; UECKER, Philip, Extraterritorial Regulatory Jurisdiction in Data Protection Law (Extraterritoriale Regelungshoheit im Datenschutzrecht). Nomos, Baden-Baden, 2017.

[115] TAYLOR, M. S. C., et al, Permissions and prohibitions in data protection jurisdiction. Brussels privacy hub working paper 2016, Vol. 2, p. 23; SVANTESSON, Dan Jerker B, The Extraterritoriality of EU Data Privacy Law - its Theoretical Justification and Its Practical Effect on US Businesses. Stanford Journal of International Law, 2014, Vol. 50, p. 85.

persons that have a stable residency status in the EU. Further, Art. 3 (2) indeed focuses more on the EU individuals rather than the territory of the EU. Thus, Art. 3 (2) shows a shift towards the passive personality principle.

3. Brief summary

To sum up, public international law allows states to exercise extraterritorial prescriptive jurisdiction based on permissive principles such as the nationality principle, the passive personality principle or the protective principle, each showing a certain connection of the subject matter to the regulating state.[116] The applicable law rules in the GDPR mainly rely on the objective territoriality principle, the effects doctrine and the passive nationality principle. Although these permissive principles are not uncontroversial, in principle they are not against the public international law.

Specifically, Art. 3 (1) GDPR can be argued to still fall partly within the least controversial territoriality principle, since it presupposes a local establishment of the data controller or processor in the EU. In so far as the CJEU has interpreted the establishment and the element of "processing carried out in the context of the activities of the establishment" so widely, that the application scope of Art. 3 (1) is factually extended, it can be argued that this part has gone beyond the territoriality principle in its strict meaning, but still has a connection to the territory of the EU. Art 3 (2) only requires that the data subjects are in the EU, the data controller or processor and the processing itself does not need to have any physical link to the EU territory. Nevertheless, the targeting approach adopted in Art. 3 (2) indicates that the data processing has an intentionally caused effect on the data subjects in the EU, thus can be backed up by the objective territoriality principle and its extension, the effects doctrine. Besides, the passive personality principle also comes into play in Art. 3 (2), but rather in a modified way, since Art. 3 (2) applies to the processing of personal data of the data subjects located in the EU, thus attaches the application of the law to the individual status but not the citizenship.

[116] RYNGAERT, Cedric, Jurisdiction in International Law. Oxford University Press, Oxford, 2015, p. 29.

Again, although extraterritorial jurisdiction is allowed for prescriptive jurisdiction, enforcement jurisdiction is however to a great extent territorial. This leads to a dilemma that a state may legislate extraterritorially but is lack of the ability to enforce its law abroad. Under the framework of the GDPR, the most problematic aspect is extraterritorial enforcement. If the GDPR applies to data processing activities carried out by a data controller or processor outside of the EU according to Art. 3, the EU has few means to enforce GDPR compliance outside its jurisdiction. Indeed, some scholars have deemed the extraterritorial enforcement a genuine issue.[117]

III. Possibilities to Enforce the GDPR in China

1. Public and private enforcement possibilities under the GDPR

The GDPR provides several possibilities to ensure the implementation and enforcement of its substantial rules in the practice. Whereas the supervisory authority can initiate investigations against data breaches, data subjects may also act spontaneously to defend their rights. In addition, representative organizations may also represent a group of data subjects to initiate a collective suit.

If a data subject suspects that his or her right to the protection of personal data has been infringed upon by a controller or processor, he or she may at his own discretion lodge a complaint to a supervisory authority or file a case to the court. Furthermore, if the data subject is not satisfied with the decision made by the supervisory authority, the data subject has a right to judicial remedy against the decision of the supervisory authority.[118] These remedy possibilities are not mutually exclusive, instead, the data subject is entitled to seek one remedy without prejudice to the other.[119] Depending on which remedy the data subject chooses, it would lead to different consequences.

The data subject's complaint to a supervisory authority leads to the exercise of

[117] GREZE, Benjamin, The Extraterritorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives. International Data Privacy Law, Vol. 9, 2019, p. 109-128.
[118] Art. 78 GDPR.
[119] Art. 77, 78, 79 GDPR.

administrative power by the competent supervisory authority, including investigation, eventually also administrative orders or fines. Further, if the data subject brings a suit against the decision of the supervisory authority to the court, it leads to a court proceeding between the data subject as a private person and the data supervisory authority as an administrative authority. This court proceeding is administrative in nature and will in principle be handled by the administrative court, if such division of court types exist in a Member State. Both the enforcement action leaded by the supervisory authority and the enforcement of an administrative court judgement should belong to public enforcement of the GDPR due to its administrative law nature.

If the data subject brings a private lawsuit against the controller or processor to the court, it results in a court proceeding between two private parties.[120] Under such circumstances, the data subject seeks remedies against a private counterparty for his or her own interest, thus, the claim of the data subject is largely considered civil in nature.[121] The same also applies to collective cases filed by a representation organization on behalf of a group of data subjects. Such litigation brought up by the data subject against the data controller or processor, principally for the purposes of compensation of damages occurred to the data subject, or suspension and correction of the violating acts, composes a private enforcement of the GDPR, primarily serving a compensatory purpose.[122]

1.1 Private Enforcement possibilities under the GDPR

In terms of the types of the claims that a data subject is entitled to make in such private court proceedings against a data controller or processor, the GDPR does not impose any particular limits on it. According to Art. 79, "each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data

[120] LUNDSTEDT, Lydia, International Jurisdiction over Crossborder Private Enforcement Actions under the GDPR, Faculty of Law. Stockholm University Research Paper, 2018, No. 57, p. 50.
[121] BRKAN, Maja, Data Protection and European Private International Law: Observing a Bull in a China Shop. International Data Privacy Law 2015, Vol. 5, No. 4, pp. 257-278.
[122] See also REICHEL, Jane; CHAMBERLAIN, Johanna, The Relationship Between Damages and Administrative Fines in the EU General Data Protection Regulation, Faculty of Law, Stockholm University Research Paper, 2019, No. 72.

in non-compliance with this Regulation." Thus, it is to assume that the data subject may initiate a court proceeding to exercise all his rights granted by the GDPR, such as the right to access, to erasure or rectification, and that the court is able to issue orders requiring the controller to fulfill such rights. Moreover, if the data subject suffers material or non-material damages from an infringement, he or she will have the right to receive compensation for the damages suffered.[123] According to Art. 82, claims to compensation could only be brought before the courts.

The private enforcement of data subject rights is, however, not without obstacles. What should first be taken into consideration is the court jurisdiction problem in private enforcement actions. The GDPR establishes a special jurisdiction rule aside of the general private international jurisdiction rules through Art. 79, which says, proceedings against a data controller or processor shall be brought to the court where the controller or processor has an establishment, or where the data subject has his or her habitual residence. This raises little problems in domestic cases, since both the two key notions, "establishment" and "habitual residence" in this jurisdiction rule, are comparatively clearly defined through the previous legislature and CJEU cases. However, uncertainties may arise in cross border matters. In this regard, a distinction should be made between cases involving only EU Member states and those involving non-EU states, since within the EU, court jurisdiction scope and enforcement matters are largely unified by the Brussels 1a Regulation and the Lugano Convention.[124]

1.1.1 Proceedings against data controllers or processors within the EU

Within the EU, the GDPR applies equally to all Member States. Thus, the aforementioned jurisdiction rule will cause little problem for cases involving several Member States. In addition, scholars have largely advocated that the jurisdiction rule in the GDPR constitutes a *lex specialis* to that in the Brussels 1a Regulation and the Lugano Convention.[125] Therefore, the general rules of the Brussels 1a Regulation and

[123] Art. 82 of the GDPR.
[124] See LUNDSTEDT, Lydia, International Jurisdiction over Crossborder Private Enforcement Actions under the GDPR, Faculty of Law. Stockholm University Research Paper, 2018, No. 57.
[125] PATO, Alexia, The Collective Private Enforcement of Data Protection Rights in the EU, available at SSRN 3303228. BRKAN, Maja, Data Protection and European Private International Law: Observing a Bull in a China Shop. International Data Privacy Law 2015, Vol. 5, No. 4, pp. 257-278.

the Lugano Convention applies in addition, whereas the aforementioned jurisdiction rule in the GDPR applies first. Besides, the Brussels 1a Regulation and the Lugano Convention also provide barrier-free recognition and enforcement of court judgements within the EU.

1.1.2 Proceedings against controllers or processors located outside of the EU

In the event that the data controller or processor is located outside of the EU, the data subject in the EU may still invoke Art. 79 GDPR to initiate court proceedings, provided the GDPR applies to the processing activities of the controller or processor located outside of the EU. In such cases, where the data subject may bring up a court proceeding is largely dependent on whether the said controller or processor has an establishment within the EU. If the data controller or processor has an establishment in the EU, irrespective of whether the processing activities are carried out in the context of that establishment, the data subject may always bring a lawsuit against the controller or processor in the Member State where the latter has its establishment.[126] Otherwise, if the data controller or processor does not have any establishment in the Member States of the EU, the only possibility remains for the data subject is to resort to the court where the data subject has his or her habitual residence.

While finding the court which has jurisdiction to the matter is not the biggest obstacle, enforcing the court judgement might be challenging. If the data controller or processor has any establishment within the EU, enforcement might be imposed on that establishment, as shown in the sanction of the French Data Protection Authority against Google LLC.[127] However, there is no guarantee that the establishment would be capable of satisfying the court's injunctive order or compensation decision. If the establishment of the data controller or processor in the EU is not able to follow the orders or decisions issued by the court, due to limited authorization or factual difficulties, such as no access or control over the data, or worse, if the data controller or processor has no establishment in the EU, even if the data subject could bring the

[126] Art. 79 GDPR.
[127] Available at: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc, last visited on 20.09.2020.

dispute to the court, it remains questionable whether the judgement resulted from such court proceedings is actually enforceable.

In the absence of bilateral or multilateral treaties, the answer to this question lies in a state's domestic rules regarding to the recognition and enforcement of foreign judgements. Given that there is no binding global convention for recognition and enforcement of foreign court judgements yet and little prospect of having one in the foreseeable future, the enforcement of EU judgement is largely dependent on the domestic law of the state where the enforcement of EU judgement is sought, as well as whether there is bilateral agreement in this respect between the EU and that state.

1.2 Public enforcement of the GDPR

As noted, when a data breach is suspected, a data subject could also lodge a complaint to the supervisory authority.[128] On the other side, the supervisory authority may also launch an investigation on its own initiative. Under such circumstances, the supervisory authority is exercising its public power against the data controller or processor mainly for administrative purposes. The procedure between the two parties, namely the supervisory authority the one side, and the private data controller or processor the other side, is thus an administrative one in nature.

Whereas the court proceedings concerning cases relating to personal data are not much different from those dealing with other cases, the supervisory authority's powers are specifically defined in the GDPR and should be complied with strictly.

The competences and powers of the supervisory authority are specified in Chapter VI of the GDPR. According to this, the supervisory authority has investigative, corrective and advisory powers.[129] Investigative powers include for example, carrying out data protection audits and obtaining access to the documents and premises of the data controller, in order to identify data breaches. Corrective powers of the supervisory authority largely appear as issuing orders and imposing administrative fines within the

[128] Art. 77 GDPR.
[129] Art. 58 GDPR.

limitations set out in Art. 83. Finally, each supervisory authority is also empowered to give advice on matters relating to the processing of personal data, as well as to authorize and approve SCCs and corporate rules for transborder data transfers. The supervisory authority may make use of these powers either on its own initiative or upon the request of a data subject.

However, the powers of the supervisory authority are limited on the territory the respective Member State, except for that of the lead supervisory authority. According to Art. 60 GDPR, the lead supervisory authority is entitled to request other supervisory authorities to provide assistance.[130] Nevertheless, the additional competence scope of the lead supervisory authority does not extend to EU third countries. As a result, the public enforcement of the GDPR by the supervisory authority similarly encounters with the enforcement obstacles in the event where the data controller or processor has no establishment within the EU.

Of course, for the more difficult latter situation, the GDPR has tried to adopt a preventative approach, by requiring controllers or processors not established in the EU to designate a representative in the EU.[131] This approach, if implemented effectively, may attribute to the enforcement against controllers or processors not established in the EU. However, although Recital 80 GDPR makes clear that "the designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor", it is rather unambiguous whether such representative shall be held directly liable for the non-compliance of the controller or processor, for instance being fined or issued administrative orders. According to the final version of the "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) adopted by the European Data Protection Board, supervisory authorities should be able to "initiate enforcement proceedings through the representative"[132], including "address corrective measures or administrative fines and penalties imposed on the controller or processor to the representative"[133]. According to this interpretation of the EDPB, the primary function of the representative in enforcement actions is to communicate between the supervisory authority, the data subject and the data controller or processor

[130] Art. 60 GDPR.
[131] Art. 27 GDPR.
[132] EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.1, 12 November 2019
[133] Ibid.

located outside of the EU. Direct liability of the representative is limited to the infringement of the representative's direct obligations set out in Art. 30 and Art. 58(1),[134] in particular the obligation to obtain a record of the processing activities.

As a consequence, the existence of a representative on behalf of the controller or processor located outside of the EU provides little help to the enforcement problem. Moreover, compared to the private enforcement initiated by private plaintiffs, supervisory authorities conducting investigations, issuing orders or administrative fines obviously reflect the public law dimension of the data protection law, thus are even more difficult to be enforced abroad due to the "public law taboo" – the general denial of states to enforce public law measures including administrative orders.

2. Recognition and enforcement of foreign civil and commercial judgements in China

As noted above, the private enforcement of EU judgement is largely dependent on the domestic law of the state where the enforcement of an EU judgement is sought, as well as whether there is a relevant bilateral agreement between the EU and that state. In China, the conditions and procedure for recognizing and enforcing foreign judgements is mainly specified in the "Civil Procedure Law of the People's Republic of China" (hereinafter referred to as the "Civil Procedure Law"). Chapter 27 "Judicial Assistance" of the Civil Procedure Law provides detailed rules for recognizing and enforcing foreign judgements. Worth noting is, since the Civil Procedure Law only applies to civil and commercial matters regarding property or personal relationships between private parties,[135] the rules discussed here merely concern to the recognition and enforcement of foreign civil and commercial judgements in China.

Recognition and enforcement of foreign civil and commercial judgements can be applied for based on international conventions, mutual treaties or in accordance with the principle of reciprocity.[136] However, till now, China has not yet concluded or

[134] Ibid.
[135] Art. 3 Civil Procedure Law.
[136] Art. 276 Civil Procedure Law.

acceded to any international treaty relating to recognition and enforcement of foreign judgements. The New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards, to which China acceded in 1987, clearly, can only be invoked to recognize and enforce arbitral awards, not court judgements.

2.1 Recognition and enforcement based on mutual judicial assistance treaties

In terms of mutual treaties, according to the Ministry of Foreign Affairs of the P.R.C., China has entered into mutual judicial assistance treaties over civil and/or commercial matters with 39 countries, including that with 12 European countries: Lithuania, Hungary, Cyprus, Greece, Bulgaria, Belgium, Spain, Ukraine, Italy, Romania, France, Poland.[137] In the example of France, the French-China judicial assistance includes serving papers or documents, assistance with investigations and recognition and enforcement of court judgements on civil and commercial matters.[138] The procedures for each type of assistance are to be determined by the domestic law of the treaty states. For the recognition and enforcement of judgements on civil and commercial matters specifically, application for recognition and enforcement of judgements must be submitted directly by the involved dispute party/parties to the court of the treaty state where recognition and enforcement is sought.[139] The competent court of the treaty state where recognition and enforcement is sought will then examine whether the judgement applied could be recognized and enforced. It is a principle that the judgement made by the court of one treaty state should be recognized and enforced in the other treaty states, with a few exceptions such as the court which made the judgement has no jurisdiction over the subject matter, illegal procedure or the judgement is prejudicial to the sovereignty, safety or public order.[140]

Whereas mutual judicial assistance treaties facilitate recognition and enforcement of foreign judgements among the treaty states, there are challenges that may weaken the outcome of such recognition and enforcement. With regard to the recognition and

[137] See http://treaty.mfa.gov.cn/Treaty/web/list.jsp, last visited on 13.02.2020.
[138] Art. 2 of the French-China Judicial Assistance Treaty, available at http://treaty.mfa.gov.cn/tykfiles/20180718/1531876617542.pdf, last visited on 13.10.2020.
[139] Art. 20 of the French China Judicial Assistance Treaty.
[140] Art. 22 of the French-China Judicial Assistance Treaty.

enforcement of EU civil and commercial judgements in China, first, not all EU states have reached a judicial assistance treaty with China. Thus, the prospect of enforcing judgement in China vary from Member State to Member State. Germany, for example, could not request enforcement of judgements made by its own court based on mutual treaty. Second, the application of recognition and enforcement must be submitted to and reviewed by a Chinese court. Moreover, the complexity of such recognition procedure makes it difficult, if possible at all, for individual data subjects located in the EU to apply for enforcement in China.

2.2 Recognition and enforcement in accordance with the principle of reciprocity

Another alternative is to recognize and enforce foreign judgements in accordance with the principle of reciprocity. However, comparing to judicial assistance based on mutual treaties, the reciprocity approach has significantly more flaws.

On one side, following the reply letter of the Chinese Supreme People's Court to a local court regarding the recognition and enforcement of a Japanese judgement in 1995,[141] Chinese courts are reluctant to make the first move to recognize foreign judgements, as can be observed in various cases, for instance Ma *vs.* Symantec[142] and a Germany company's application in 2001 for the enforcement of a German judgement in China[143]. Recently, along with the "One Belt, One Road" initiative, the Chinese Supreme People's Court has issued a range of instructions to enable a more proactive recognition and enforcement of foreign judgements by Chinese courts.[144] This removes some obstacles for a more flexible, effective recognition and enforcement of foreign judgements in China. However, even after this transition of altitude of the Supreme People's Court, no Chinese court has ever invoked the principle of reciprocity to first recognize and enforce foreign judgements in the event that non-Chinese judgement has

[141] Supreme People's Court, Reply Letter on Whether the People's Court of China Should Recognize and Enforce the Judgment of Japanese Courts Over Contractual Issues, 26.06.1995.

[142] Ma *vs.* Symantec, (2011) 沪高民三（知）终字第 88 号，the Superior People's Court of Shanghai, 8.04.2012.

[143] MA, Mingfei (马明飞); CAI, Siyang (蔡斯扬), The Reciprocity Principle in the Recognition and Enforcement of Foreign Judgments in China (我国承认与执行外国判决中的互惠原则). Political Science and Law (政治与法律), 2019, Vol. 3, P. 14.

[144] Such as, Supreme People's Court, "Some Opinions on the Judicial Services and Guarantees provided by the People's Court for the One Belt and One Road", 16.06.2015, available at http://gongbao.court.gov.cn/Details/b10a1d30141bc4a4c7886b00d759c3.html.

been recognized and enforced by the courts of the foreign state involved.

On the other side though, there is a clear trend of Chinese court more and more actively recognizing and enforcing foreign civil and commercial judgements, when the foreign state involved has a record of recognizing Chinese judgements. For instance, the Intermediate People's Court of Nanjing has recognized a judgement made by the Singapore High Court in 2016, based on the argument that the Singapore High Court had enforced a civil judgement made by the Intermediate People's Court of Suzhou in 2014.[145] Later on, in 2017, the Intermediate People's Court of Wuhan recognized another commercial judgement made by an American court in California invoking the same reason.[146]

Thus, for EU states that do not have a mutual judicial assistance treaty with China, such as Germany, civil or commercial judgements made by a local court may have a brighter chance to be recognized and enforced in China, if courts in that country have recognized and enforced judgements made by Chinese courts before. In fact, the Superior Court of Berlin (Kammergericht) already recognized a commercial judgement made by the Intermediate People's Court of Wuxi in 2006,[147] with an explicit hope of the ruling court to create a reciprocity relationship with China.[148]. Later on, this kind gesture of the berlin Superior Court was repaid by the Intermediate People's Court of Wuhan in 2013 in a bankruptcy case. In that case, the Intermediate People's Court of Wuhan recognized and enforced a commercial judgement made by the German Local Court of Montabaur based on reciprocity between Germany and China.[149] There is, however,

---

[145] Kolmar Group AG *vs.* Jiangsu Textile Group, (2016) 苏 01 协外认 3 号, Intermediate People's Court of Nanjing, 09.12.2016.

[146] Liu Li *vs.* Tao Li, Dong Wu, (2015) 鄂武汉中民商外初字第 00026 号, Intermediate People's Court of Wuhan, 30.06.2017.

[147] Court of Appeal Berlin, 20 SCH 13/04, 18.05.2006.

[148] Court of Appeal Berlin, 20 SCH 13/04, 18.05.2006, Reason 17 "In the absence of an international agreement between the Federal Republic of Germany and the People's Republic of China on the mutual recognition of judgments, the actual handling is decisive. Since in such cases one side would have to start with recognition before the other could follow suit, this would de facto exclude mutual recognition, which is not what the legislator intended. Therefore, in order not to block the development of mutual recognition without the conclusion of international treaties, the focus should be on whether it can be expected that the other side will follow suit (Grund 17 "Mangels internationaler Vereinbarung zwischen der Bundesrepublik Deutschland und der Volksrepublik China über die gegenseitige Anerkennung von Urteilen ist die tatsächliche Handhabung maßgeblich. Da in solchen Fällen eine Seite mit der Anerkennung beginnen müsste, bevor die andere nachziehen könnte, würde das die gegenseitige Anerkennung faktisch ausschließen, was so vom Gesetzgeber nicht gewollt ist. Deshalb ist, um die Entwicklung gegenseitiger Anerkennung ohne Abschluss internationaler Verträge nicht zu blockieren, darauf abzustellen, ob zu erwarten ist, dass die andere Seite nachziehen wird").

[149] Sascha Rudolf Seehaus, (2012) 鄂武汉中民商外初字第 00016 号, 26,11,2013.

until now only this one case supporting the existence of reciprocity between Germany and China. Given that precedent has no binding effect in China, and that the only court judgement aforementioned is made a provincial court, it is still to be seen whether this precedent will be followed by other courts or confirmed by the Supreme People's Court.

2.3 Brief summary

It can be observed from above that, first, both mutual treaties and reciprocity only enable a small group of the EU Member States to have their court judgements recognized and enforced in China. Under data protection law, the GDPR is a regulation which applies equally in all Member States. It is obviously not satisfying that the prospect of enforcing the data subject's rights through private enforcement is dependent on mere coincidence, namely in which Member State the data subject locates, or the data controller or processor has its establishment. This will also cause side effects similar to "forum shopping", which means, a Chinese data controller or processor might choose to establish an establishment in a Member State which has no treaty and no reciprocity relationship with China, so that the enforcement of the GDPR is basically impossible.

Second, even for EU Member States that have mutual treaties or a reciprocity relationship with China, the exceptions to recognition and enforcement of foreign judgements are rather wide and vague. These include such as prejudice to sovereignty, safety or public order. Third, the efforts for filing an application in China are prohibitively unaffordable for a natural person. This excessive burden might directly cause malfunction of the private enforcement mechanisms, in the cases where the violating data controller or processor has no establishment within the EU, or the establishment does not have enough competences or assets to be enforced. As a consequence, the desirable extraterritorial effect of Art. 3 (2) GDPR, in particularly, could not be reached by private enforcement of the GDPR.

3. Administrative investigation and enforcement actions by the data supervisory authority in China

It is well recognized that investigation activities conducted by state authorities as well as enforcement of administrative decisions or judgements are limited within a state's own territory. Investigating or enforcing administrative decisions or judgements on the territory of a foreign state without the consent of the latter would infringe the sovereignty of that foreign state, thus, it is prohibited under public international law.[150] It is not much different for China in this regard, investigation carried out by foreign administrative authorities on the Chinese territory is not allowed. Administrative decisions or court judgements cannot be enforced in China due to the lack of any mutual assistance treaties on administrative matters.

4. Alternative: market destruction measures

Extraterritorial enforcement of the GDPR against a data controller or processor located abroad is largely impossible because the involved data controller or processor has no organizations or assets enforceable within the EU, and a direct enforcement on the territory of a foreign state is not allowed. However, as Jack Goldsmith correctly observed, "a nation can take many steps within its territory to regulate content transmitted from abroad indirectly".[151]

One possibility to consider is to adopt market access measures, or what are called "market destroying measures" by Dan Jerker B. Svantesson.[152] Such measures were originally discussed as a tool to enforce internet related regulations that have an overreaching scope but are almost impossible to be enforced due to its extraterritorial characteristic.[153] Facing the same enforcement dilemma, this tool could also serve the purpose of solving enforcement difficulties occurred in the field of data protection, particularly in the online context. The key of market destroying measures is to influence

[150] KAMMINGA, Menno, Extraterritoriality. Max Planck Encyclopedias of International Law, 2012, p. 1070-1077.
[151] GOLDSMITH, Jack. Unilateral Regulation of the Internet: A Modest Defence. European Journal of International Law, 2000, Vol. 11, No. 1, pp. 135-148.
[152] SVANTESSON, Dan Jerker B, The Extraterritoriality of EU Data Privacy Law - its Theoretical Justification and Its Practical Effect on US Businesses. Stanford Journal of International Law, 2014, Vol. 50, p. 53.
[153] Ibid.

the conduct of the party located abroad through regulating domestic factors, in worst cases even to block the access of the party located abroad to the domestic market. For instance, in online copyright cases, measures like blocking website are already taken by some Member States.[154] Moreover, there are already news reporting US companies using Geo-blocking to block access of the EU users, in order to avoid application of the GDPR.[155] Since businesses can use this kind of technique to disconnect with the GDPR, it seems reasonable that regulators also use this to punish those who desire to enter the EU market but refuse to pay the compliance costs.

The drawbacks of the market destroying measures are, however, also not negligible. First, unlike in other fields such as in the intellectual property area, where both the producer abroad and the domestic importer are at fault for the infringement of an intellectual property, under the data protection, only the data controller and/or processor should be responsible for the data breaches, so that a transition of burden to other domestic partners in order to impose indirect pressure on the data controller and/or processor abroad is lack of legal basis. Further, the powers granted to the supervisory authorities as by Art. 58 GDPR do not include the ordering of denying market access, for example via blocking web access. In this case, denying market access should only come into question, if the data controller or processor located in the third country has refused to cooperate with the corrective measures or fines issued by the data protection supervisory authority in accordance with Art. 58 GDPR. Due to the fatal consequences of such market destruction measures, and just like any other law enforcement measures, there must be due judicial procedural safeguards to protect the lawful rights of the party subject to the enforcement, such as with a court order. Currently, such procedures do not appear to be developed regarding data protection matters. The fact that the ordering of market destruction measures would have a collateral impact on the users, since users would not be able to access the website within the jurisdiction in which the order applies, makes the existence of a due process even more necessary.

It also remains unclear to what extent the market destruction measures should be

[154] LINDSAY, David, Website Blocking Injunctions to Prevent Copyright Infringements: Proportionality and Effectiveness. The University of New South Wales Law Journal, 2017, Vol. 40, p. 1507.
[155] For example, an article on the Econsultancy claims that several US websites have blocked EU'users access, see SENTENCE, Rebecca. Websites are Blocking Visitors From the EU? 31 May 2018, available at: https://econsultancy.com/gdpr-which-websites-are-blocking-visitors-from-the-eu-2/, last visited on 23.11.2020.

applied - will the failure of the website operator in the third country to comply with any obligation under the GDPR already lead to the blocking of the website, or will only serious breaches of the GDPR lead to the application of such measures. In this regard, the case law of the CJEU and the ECtHR rather suggests for a very careful utilization of website blocking, since the fundamental right of the users to freedom of expression and information under Article 11 of the EU Charter of Fundamental Rights and Article 10 of the European Convention on Human Rights is at stake.[156] In any case, the justification for blocking websites is overshadowed by a lack of clarity in both legal basis and due process.

In addition, denying market access might also cause conflict between states and intensify doubts about the extraterritorial claims of the GDPR, due to the harsh unilateral nature of the enforcement itself.

5. Mid-conclusion

The GDPR applies to a wide range of data controllers or processors that are not located in the EU per Art. 3, in order to ensure a sufficient protection of the fundamental rights and freedoms of the natural persons in the EU, in an era where businesses can be conducted borderless with the help of the internet. This wide application is criticized by some scholars as extraterritorial and overreaching. However, the scholarly studies have showed that the extraterritorial prescriptive (legislative) jurisdiction embedded in the GDPR is rather justified under public international law, even if not without controversy. The real problem is the dilemma between the wide application scope claimed by the GDPR and its enforcement.

This enforcement problem exists, unsurprisingly, also in the EU-China interrelationship. Even though the data processing activities of a Chinese data controllers or processors would be subject to the GDPR, if the conditions laid down in Art. 3 GDPR are fulfilled, the enforcement of the GDPR in China faces significant challenges. In this sense, the wide application scope of the GDPR per Art. 3 inherently has shortcomings in its

[156] See for example, CJEU, C-314/12, UPC Telekabel, 27.03. 2014.

enforceability, so that Art. 3 itself alone could not provide a satisfying protection level to the natural persons with regard to their personal data, when these personal data is collected or sent to the data controllers or processors located outside of the EU.

Chapter 3 The Concept and Legal Basis of Data Transfer under the GDPR

Chapter 2 has come to the conclusion that Art. 3 itself alone could not provide sufficient protection to the natural persons in the EU with regard to their personal data, when these personal data are collected or sent to the data controllers or processors located outside of the EU. In addition to expanding the application scope to data controllers or processors outside of the EU per Art. 3, another mechanism in the GDPR aims to secure a sufficient level of data protection of the EU data subjects in a third country is the data transfer rules laid down in Chapter V GDPR. This chapter will assess whether the data transfer rules in the GDPR apply to the data flows scenarios identified under the cross-border E-Commerce in chapter 1 in this dissertation, and whether these rules could contribute to the general goal of ensuring a sufficient level of data protection of the EU data subjects in a third country.

I. The Definition of Data Transfer Within the Meaning of Chapter V GDPR

Under the GDPR, any transfer of personal data to a third country or international organization must fulfill the conditions laid down in Chapter V before taking place.[157] However, previous to assessing whether these conditions are complied with, a preliminary question is whether a data transfer exist, or what constitutes a data transfer to a third country or international organization. This question is basic yet highly complicated and controversial both in the theory and practice. The GDPR itself contains no legal definition to "data transfer". During the data protection reform which results in the promulgation of the GDPR, the European Data Protection Supervisor[158] ("EDPS") has suggested to define this concept in the future GDPR,[159] however, this suggestion was not made into reality. Trying to make an own definition to the concept would be extremely difficult, when not impossible. This dissertation tries to provide a

[157] Art. 44 GDPR.
[158] The EU Data Protection Supervisor is an EU institution established in 20014 to ensure that EU institutions and bodies respect the right to the protection of personal data when they processing personal data.
[159] EDPS, Opinion of the European Data Protection Supervisor of 7 March 2012 on the data protection reform package, 7 March 2012, p. 18.

comprehensive review of the concept by analyzing the main elements that make up the concept, so that a better clarification and limitation of the concept can be achieved.

1. Transfer: the act element

Although the GDPR does not provide a definition to data transfer, there is another notion that is related to data transfer, namely the definition of processing. Processing is generally referred to as "any operation or set of operations which is performed on personal data or on sets of personal data", including "disclosure by transmission, dissemination or otherwise making available".[160] Disclosure of personal data means to provide knowledge or the possibility of knowledge to the recipient, as a result, the number of the subjects which has the knowledge multiplies.[161] Further, as a form of disclosure, "transmission" is referred to as the direct disclosure of personal data to certain recipients, while dissemination is the disclosure to uncertain recipients, and otherwise making available is an overall concept that includes all other types of disclosure, in particular the preparation for access by uploading the personal data to the internet.[162] Literally, "transmission" as a form of disclosure seems to be very similar to the meaning of transfer. In the German version of the GDPR, "transmission" and "transfer" is even translated into the same word: "Übermittlung".[163]

Against this background, in the German literature, there are different opinions in terms of whether transfer under Chapter V GDPR equals transmission under Art. 4 (2). Some German commentators hold the opinion that since the English version uses two different terms in the two positions, these two different terms should be understood differently. Thus, transfer is not identic to transmission. Transfer is not a subcategory of disclosure either, but an autonomous concept under chapter V GDPR that generally refers to every form of disclosure of personal data to the recipient(s) in a third country or international organization.[164] On the other side, other commentators understand

[160] Art. 4 (2) GDPR.
[161] REIMER, Philipp, Art. 4, in: SYDOW, Gernot, EU GDPR (Europäische Datenschutzgrundverordnung). Nomos, 2nd Edition 2018, p. 68.
[162] REIMER, Philipp, Art. 4, in: SYDOW, Gernot. EU GDPR (Europäische Datenschutzgrundverordnung). Nomos, 2nd Edition 2018, p. 69.
[163] Art. 4 (2) and Art. 44 of the GDPR (German version).
[164] GABE, Detlev, Art. 44, in: TAEGER, Jürgen; GABEL, Detlev, GDPR-German Data Protection Act (DSGVO-BDSG). Specialist Media Law and Economics, 3rd Edition 2019, p. 10; JUAREZ, Tavares, Art. 44, in: WOLFF;

transfer as identical to transmission in accordance with the German version of GDPR. Pursuant to this opinion, transfer is a subcategory of the disclosure, meaning direct disclosure of personal data to certain recipients, thus, the preparation for access by uploading of personal data to the internet is not yet a data transfer, but only when an internet user in a third country requests the personal data.[165]

Unfortunately, on the EU level, there is neither opinion from the Art. 29 Working Party, nor guideline from the EDPB specifically dealing with the definition of transfer. Only the EDPS issued one position paper concerning "the Transfer of Personal Data to Third Countries and International Organizations by EU Institutions and Bodies"[166] that has dealt with the concept of transfer. It has noted that the term transfer usually implies the "communication, disclosure or otherwise making available of personal data".[167] The EDPS further listed several examples of data transfers: sending a post or e-mail to a non-EU recipient, "push" of the data to a non-EU recipient, "pull" (granting access of) data to a non-EU recipient, direct on-line collection by a non-EU processor on behalf of an EU data controller, publication of data on the internet by an EU controller.[168] Thus, it seems like the EDPS prefers a more broad interpretation of the term transfer. According to the EDPS, transfer includes every form of disclosure, either by transmission, dissemination or otherwise making available of personal data.

This broad interpretation in the literature and by the EDPS is however not complete in line with the case law of the CJEU, at least regarding the circumstance where an individual makes personal data available on the internet. In the landmark case *Lindqvist,*[169] the CJEU seems to have denied that making personal data available on the internet by an individual through a hosting provider constitutes a data transfer with a three-stage argumentation. First, the court noted that the personal data concerned are

---

BRINK; v. UNGERN-STERNBERG, BeckOK Data Protection Law (Datenschutzrecht). BeckOK Online-Commentary, 35. Edition, p. 15; also SCHRÖDER, Christian, Art. 44, in: KÜHLING, Jürgen; BUCHNER, Benedikt. GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 2nd Edition 2018, p. 16; PAULY, Daniel A, Art. 44, in: PAAL, Boris P.; PAULY, Daniel A, GDPR German Data Protection Act (DS-GVO BDSG), C.H. BECK, 3rd Edition 2021, p. 5; ZERDICK, Thomas, Art. 44, in: EHMANN, Eugen; SELMAYR, Martin, General Data Protection Regulation (Datenschutz-Grundverordnung). C.H.BECK, 2nd Edition 2018, p. 7.

[165] HERBST, Tobias, Art. 4 (2), in: KÜHLING, Jürgen; BUCHNER, Benedikt. GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 2nd Edition 2018, p. 30-31; REIMER, Philipp, Art. 4, in: SYDOW, Gernot, EU GDPR (Europäische Datenschutzgrundverordnung). Nomos, 2nd Edition 2018, p. 69-70.

[166] EDPS, The Transfer of Personal Data to Third Countries and International Organizations by EU Institutions and Bodies, 14 July 2014, p. 7.

[167] Ibid.

[168] Ibid.

[169] CJEU, C-101/01.

not directly transferred from the controller in the EU to recipients in a third country, the controller in the EU only uploads the data to a hosting provider which locates in the EU.[170] Based on this observation, the court then analyzed whether it was the legislator's intention to include such uploading of personal data onto an internet page as a data transfer. Taking into consideration of the issuing date of the Data Protection Directive and the absence of criteria applicable to the internet, the court came to the conclusion that it cannot be assumed that the above-mentioned scenario should be considered as a data transfer to a third country.[171] Last, if a data transfer to a third country exists in such case, the data transfer mechanism in the EU data protection law would apply to operations on the internet generally, which was not the intention of the legislator concerning cross-border data transfer.[172] Thus, in this very specific case, the CJEU has concluded that loading personal data onto an internet page hosted by a provider established within the EU, thus making that data accessible to anyone having access to the internet, including people in a third country, is not a "data transfer to a third country".

However, the ruling is the result of an array of specific circumstances in the presented case. The case cannot be interpreted in a way that no data flow from the EU to a third country through the internet is a data transfer within the meaning of chapter V GDPR. The Lindqvist case only concerns one scenario of uploading personal data onto an internet page for access, in which the uploading act by the data controller within the EU is separated from the access act by the recipient in a third country, with a hosting provider as intermediary. If, however, a data subject within the EU directly sends data to the server of the recipient on the internet, the court's separation between the uploading and accessing act would not exist. As a result, the data is transferred between the two parties, and there is no risk of application of the data transfer rules in the GDPR to all third countries, thus, a data transfer may well exist. In other words, in cases where the concern of general application of the data transfer regime on the whole internet does not exist, loading data on the internet may still be deemed as a data transfer.

[170] CJEU, C-101/01, para. 61.
[171] Ibid, para. 68.
[172] Ibid, para. 69.

2. The intention to disclose personal data to recipients in a third country

In the *Lindqvist* case, the CJEU did not explicitly discuss whether the intention of the data controller within the EU (Ms. *Lindqvist* in that case) to allow third country entities to access the uploaded personal data is relevant for the existence of a data transfer to a third country. However, commentators usually consider the intention or at least the knowledge of the transferor, that the personal data may be accessed by recipients in a third country, an important element of the data transfer concept.[173] In the *Lindqvist* case, Ms. *Lindqvist* only intends to disclose the personal data of her colleagues to the local people, not to recipients in a third country.[174] Thus, an intention to disclose personal data to recipients in a third country is absent in the case. On the contrary, if Ms. Lindqvist uploads personal data to an internet page with the specific intention to grant access to recipients in a third country, there is no reason why this should not constitute a data transfer, at least there should be a data transfer to the intended recipients in that third country. Just like some commentators argued, it makes no sense why intentionally making available personal data to the whole world is not a transfer to a third country, while transferring to a specific recipient in a third country constitutes a transfer.[175] Thus, in any case, if there is an identified intention of the data controller to make personal data available to recipients in a third country, there should be a data transfer.[176] On the contrary, if such an intention is absent, like in the Lindqvist case, other elements must be considered such as whether it would lead to the application of the data transfer rules to the whole internet.

3. The transferor and recipient

Another controversial question concerning data transfer to a third country or

---

[173] ESAYAS, Samson Yoseph, A walk in to the Cloud and Cloudy It Remains: The Challenges and Prospects of "Processing" and "Transferring" Personal Data. Computer Law & Security Review, 2012, Vol. 28, No. 6, p. 670; HON, W. Kuan; MILLARD, Christopher, Data Exports in Cloud Computing-How Can Personal Data be Transferred outside the EEA? The Cloud of Unknowing, Queen Mary School of Law Legal Studies Research Paper 2011, No. 85, p. 35.
[174] CJEU, C-101/01, para. 12.
[175] ESAYAS, Samson Yoseph, A walk in to the Cloud and Cloudy It Remains: The Challenges and Prospects of "Processing" and "Transferring" Personal Data. Computer Law & Security Review, 2012, Vol. 28, No. 6, p. 670.
[176] Ibid.

international organization is the determination of the transferor and the recipient. In other words, who is the data exporter and who is the data importer, and more specifically, what are their respective responsibilities.

The wording of Chapter V GDPR does not provide much elaboration regarding this issue, it only imposes the obligation to comply with the conditions laid down in Chapter V on the controller and processor.[177] Art. 46 further specifies that in the absence of an adequacy decision, a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards.[178] This indicates that the obligations are primarily imposed on the exporting controller or processor. However, it still leaves several questions open, such as whether the exporting controller or processor must be located within the EU, since according to Art. 3 section 2 GDPR, under certain circumstances non-EU data controllers can be subject to the GDPR too. Another question is when the data exporter is a processor, whether Chapter V GDPR only applies to the data transfer from that processor to a sub-processor or also to a non-EU controller. Further, it is somewhat controversial too whether the data subject itself could act as an exporter to transfer its own data outside of the EU. Against this background, it is helpful to explore whether the concept "transfer" within the meaning of Chapter V GDPR contains or indicates any conditions for the status of the transferor and recipient, so that only data sent by a specific type of transferor to a specific type of recipient in a third country would be deemed as data transfers under Chapter V GDPR.

3.1 Data controller as transferor: controller to controller and controller to processor

A data controller established in the EU sends personal data to a recipient in a third country is probably the most typical scenario of data transfer to a third country. The recipient in the third country can be another controller or a processor. However, even in this seemly unambiguous scenario, there are an array of unanswered questions that

[177] Art. 44 GDPR.
[178] Art. 46 GDPR.

covers the data transfer with dark clouds. In the following two special circumstances under this scenario will be discussed.

It is provided in Art. 4 (9) GDPR that a recipient is a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, irrelevant of it being a third party or not.[179] A third party is any natural or legal person that is not the data subject, controller, processor and persons who process personal data under the direct authority of the controller or processor.[180] According to these two definitions, since it is not stated that the recipient has to be a third party, thus, it can also be the processor, the data subject or even a person or dependent internal organ within the controller itself. However, this literal interpretation is partially restricted in the literature.[181]

Commentators argue that the employees or dependent internal organs within the controller within the EU should not be deemed as recipients within the meaning of Art. 4 (9), because recipients must have a certain degree of independence,[182] and must be able to assume legal responsibilities against the data subject.[183] Obviously, the employees and dependent internal organs usually do not meet these requirements.

In contrast, if personal data are transferred from an EU controller to a dependent branch located in a third country, a data transfer should exist according to most commentators.[184] The reason behind this should be the extra risks brought by the location of the personal data in a third country after the transfer.[185] In any case, personal data transferred by a corporate affiliate to another corporate affiliate in a third country within the same company group is considered a data transfer to a third country, since it

---

[179] Art. 4 (9) GDPR.
[180] Art. 4 (10) GDPR.
[181] ARNING; ROTHKEGL, Art. 4, in: TAEGER, Jürgen; GABEL, Detlev, GDPR-German Data Protection Act (DSGVO-BDSG). Specialist Media Law and Economics, 3rd Edition 2019, p. 238; SCHÖTTLE, Hendrik, III. Internationaler Datentransfer, in: WETH, Stephan; HERBERGER, Maximilian; WÄCHTER, Michael, Data and Personality Protection in the Employment Relationship (Daten- und Persönlichkeitsschutz im Arbeitsverhältnis). C.H. BECK, 2nd Edition 2019, p. 14; ERNST, Stefan, Art. 4, in: PAAL, Boris P.; PAULY, Daniel A, GDPR German Data Protection Act (DS-GVO BDSG), C.H. BECK, 3rd Edition 2021, p. 57; GOLA, Peter, Commentary on the GDPR (DS-GVO), C.H. BECK, 2nd Edition 2018, p. 63.
[182] ERNST, Stefan, Art. 4, in: PAAL, Boris P.; PAULY, Daniel A, GDPR German Data Protection Act (DS-GVO BDSG), C.H. BECK, 3rd Edition 2021, p. 57
[183] ARNING; ROTHKEGL, Art. 4, in: TAEGER, Jürgen; GABEL, Detlev, GDPR-German Data Protection Act (DSGVO-BDSG). Specialist Media Law and Economics, 3rd Edition 2019, p. 238.
[184] For example, SCHÖTTLE, Hendrik, III. Internationaler Datentransfer, in: WETH, Stephan; HERBERGER, Maximilian; WÄCHTER, Michael, Data and Personality Protection in the Employment Relationship (Daten- und Persönlichkeitsschutz im Arbeitsverhältnis). C.H. BECK, 2nd Edition 2019, p. 14.
[185] Ibid.

is the major target group of the binding corporate rules.

3.2 Data processor as transferor: processor to controller or processor to sub-processor

Compared to the outdated Data Protection Directive, the GDPR now explicitly lays down that a processor could also act as a data exporter that transfers personal data to a third country or international organization.[186] Nevertheless, an unsettled question further remains as whether Chapter V GDPR applies to all circumstances where the exporting processor disclose personal data of EU data subjects to a recipient in a third country. More specifically, it is not clear whether the data transfer from an EU processor to the data controller to whose instructions the exporting processor is subject or another data controller is considered as a data transfer within the meaning of Chapter V GDPR, or it must be interpreted as Chapter V only applies to the case where the EU data processor transfers personal data to a sub-processor.

3.2.1 Processor to controller that is subject to the GDPR

If a non-EU data controller engages a processor within the EU to process personal data of EU data subjects, the EU processor might need to transfer the preliminary processed personal data back to the non-EU controller. Whether such transfer is subject to the conditions laid down in Chapter V GDPR for data transfer to a third country is not always clear.

a. Legal status under the Data Protection Directive

As noted above, under the Data Protection Directive, only the data controller is the addressee of the data transfer rules under Chapter IV. At that time, data flow from a EU processor to a non-EU data controller was not considered a data transfer under the Data

[186] Art. 46 section 1 GDPR.

Protection Directive. In Germany, the Düsseldorfer Kreis,[187] a coordination body of the German data protection supervisory authorities, issued a non-binding guidance with regard to the cross-border data processing, in which it analyzed the application of the data transfer rules in various case groups.[188] This guidance of the Düsserdorfer Kreis stated that a data processor within Germany (EU/EWR) is not obliged to ensure that the transfer of personal data to the non-EU data controller meets the data transfer rules laid down in the German data protection law.[189] According to the Düsserdorfer Kreis, this is because the processor within Germany (EU/EWR) lacks the ability to conduct a comprehensive compliance check in terms of the data processing in general, since it is only the processor and usually does not have all information relating to the whole data processing.[190] Besides, the non-EU data controller itself is subject to the German Data Protection Law, it is this non-EU data controller that assumes responsibilities for complying with the general conditions laid down for the data processing, not the data processor.[191]

b. Legal status under the GDPR

Under the GDPR, Chapter V now explicitly also imposes the obligation to comply with the data transfer rules on the processor. As a result, one of the two above-mentioned arguments of the Düsserdorfer Kreis denying the obligation of the EU processor in this respect does not apply any more. The literal meaning of Chapter V rather supports the existence of such an obligation for the EU data processor. Nevertheless, the dispute concerning to this question has not stopped.

Some scholars hold that the EU data processor has to make sure that the conditions for data transfer to a third country are met, when it transfers personal data of EU data subjects to the non-EU controller under whose instructions the data are processed.[192]

---

[187] The Düsseldorfer Kreis is a working group under the Data Protection Conference held regularly to discuss data protection issues, attended by German federal and state data protection supervisory authorities responsible for data protection supervision in private domain. It is named after the head meeting location of the conference.
[188] Düsseldorfer Kreis, Guidance from the Düsseldorfer Kreis on the Legal Assessment of Case Groups for International Commissioned Data Processing (Handreichung des Düsseldorfer Kreises zur rechtlichen Bewertung von Fallgruppen zur internationalen Auftragsdatenverarbeitung), 28.03.2007.
[189] Ibid, p. 15-16.
[190] Ibid, p. 15.
[191] Ibid, p. 16.
[192] HORNUNG, Gerrit, Art. 3, in: SIMITS, S.; HORNUNG, G.; SPIECKER gen. DÖHMANN, I, Data Protection

The reasons according to them are firstly, neither the wording of Chapter V for data transfer nor the provisions related to data processors provides a privilege for the data flows from the processor to the controller. Secondly, even if the personal data was originally received from the data controller, the data processor has most probably altered it or combined it with other data, so that the personal data transferred back to the controller is not the same.[193] Other commentators are of the opinion that the EU data processor's obligation to comply with the conditions for data transfer to a third country should be restricted to the processor transferring data to a sub-processor.[194] Though these commentators realize that the wording of Chapter V GDPR now generally puts the obligation to comply with the restrictions for data transfer to a third country on the processor too, they deem it more reasonable to restrict this obligation to the scenario data transfer from processor to sub-processor, however without providing further arguments other than referring to the argument made by the Düsseldorfer Kreis above.[195]

3.2.2 Data processor to data controller that is not subject to the GDPR

If the non-EU controller itself is not subject to the GDPR, but engages a data processor within the EU to process personal data for him, the involved personal data may be not related to an EU data subject at all, and the link between the data processing and the EU is rather very weak. The position that the EU data processor still has to comply with the restriction for data transfer to a third country in such case appears at first very unconvincing due to the weak link between the personal data and the EU.[196]

The 3/2018 guidelines from the European Data Protection Board ("EDPB") have

---

Law (Datenschutzrecht), Nomos, 1st Edition 2019, p. 34; SCHANTZ, Peter, Art. 44, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, p. 12.

[193] HORNUNG, Gerrit, Art. 3, in: SIMITS, S.; HORNUNG, G.; SPIECKER gen. DÖHMANN, I, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, p. 34.

[194] KLAR, Manuel, Art. 3, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 38; SCHRÖDER, Christian, Art. 46, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 21; GABEL, Detlev, Art. 44, in: TAEGER, Jürgen; GABEL, Detlev, GDPR-German Data Protection Act (DSGVO-BDSG). Specialist Media Law and Economics, 3rd Edition 2019, p. 38.

[195] Ibid.

[196] See also SCHRÖDER, Christian, Art. 46, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 21.

specifically dealt with this circumstance.[197] It makes clear that the mere fact that the processor is in the EU does not trigger the application of the GDPR to the non-EU data controller, meanwhile, the processor itself must comply with the relevant GDPR provisions applicable to data processors.[198] These provisions applicable to the data processors include the provisions on transfer of personal data to third countries or international organizations as per Chapter V.[199] Thus, according to the EDPB, even if the non-EU data controller is not subject to the GDPR, the transfer of personal data from the engaged processor within the EU to the non-EU data controller still has to meet the restrictions for data transfer under Chapter V GDPR. This reflects the reinforcement of the data processor's obligations under the GDPR. However, it also raises the question whether this is contradictive to the EDPB's position that the non-EU data controller should not be subject to the GDPR merely because it engages a data processor within the EU, since the application of data transfer rules to the processor inevitably means the non-EU data controller will also have to comply with some of the GDPR obligations, at least contractually.[200]

3.2.3 Processor to sub-processor

That data flow from an EU processor to a sub-processor constitutes a data transfer, thus must meet the restrictions for data transfer to a third country is not much disputed. Even the scholars that are against the application of Chapter V to data flows from a EU processor to a non-EU controller recognize the application of Chapter V to data transfer from an EU processor to a non-EU sub-processor.

3.3 Transfer directly by the data subject to a recipient outside of the EU

The question, whether it constitutes a data transfer to a third country, when personal

[197] EDPB, Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) Version 2.1, 07 January 2020.
[198] Ibid, p. 13.
[199] Ibid.
[200] MILLARD; KAMARINGOU, Art. 28, in: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher, The EU Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 1st Edition 2020, pp. 948-949.

data are disclosed to a recipient located in a third country directly by the data subject itself, remains controversial. The GDPR, the opinions of the Art. 29 working party as well as the guidelines of the EDPB do not provide clarity on this specific circumstance. In the literature, there are opposing opinions towards this question.

3.3.1 Con

Some scholars hold that an EU data subject sending his or her own data to a recipient in a third country does not constitute a data transfer to a third country within the meaning of Chapter V GDPR.

First, Art. 46 only addresses the "controller or processor" as transferor, not the data subject itself.[201] Thus, the data subject is not a transferor within the meaning of chapter V GDPR. In the here discussed case of a data subject disclosing personal data to a recipient in a third country, there is no controller or processor within the EU, but only the data subject itself. However, it must be further considered whether the non-EU data controller could act as a transferor, since it is the non-EU controller that requires the data subject to input the data, it is also the non-EU controller that decides where the personal data should be sent. The question then transformed into, whether a non-EU data controller or processor is the eligible transferor within the meaning of Chapter V GDPR. The wording of Art. 46 and other provisions under Chapter V does not provide a clear answer to this question. Some commentators have argued that Chapter V only applies when there is a controller or processor within the EU.[202]

Another argument is that, such disclosure will fall under the territorial scope of the GDPR per Art. 3 (2), if the conditions set down therein are met. As a result, the GDPR would apply to the recipient (i.e. the non-EU data controller). Against this background,

---

[201] VOIGT, Paul, Art. 49, in: SPINDLER, Gerald; SCHUSTER, Fabian, Electronic Media Law (Recht der elektronischen Medien). C.H.Beck, 4th Edition 2019, p. 4; VOIGT, Paul, Requirements for Third Country Transfers-Unresolved Issues (Anforderungen an Drittlandtransfers-ungeklärte Fragen). Computer und Recht, 2020, Vol. 36, No. 5, p. 319.

[202] VOIGT, Paul, Art. 49, in: SPINDLER, Gerald; SCHUSTER, Fabian, Electronic Media Law (Recht der elektronischen Medien). C.H.Beck, 4th Edition 2019, p. 4; KUNER, Christopher, European Data Privacy Law and Online Business. Oxford University Press, Oxford, 2003, p. 120; See SCHANTZ, Peter, Art. 44, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, p. 15.

it is argued that since the GDPR already applies to the non-EU data controller in the third country, an appropriate level of protection is already guaranteed, so that the application of Chapter V with its additional conditions is redundant.[203]

3.3.2 Pro

In contrast to the position above, there is an opposing opinion advocating that disclosure of personal data by the data subject to a recipient in a third country constitutes a data transfer to a third country within the meaning of chapter V GDPR.

It is argued that Chapter V regulating data transfer to a third country imposes certain obligations on the data controller or processor, irrelevant of whether the data controller or processor is the exporter or importer.[204] In addition, Art. 44 explicitly applies to transfer of "personal data that are intended for processing after transfer to a third country", which is exactly the case discussed here.[205] If the restrictions for data transfer to a third country are not applicable in this scenario, there would be a loophole of the protection to the EU data subjects. This is because the direct collection and transfer of personal data of the EU data subjects by a non-EU data controller does not cause less risk for the EU data subjects as in the case, where personal data are collected by a EU data controller first and then transferred to a third country. Thus, the need for adding another layer of protection through the data transfer rules under Chapter V still exists.[206]

Another argument of the con-side is that the GDPR already applies to the data controller outside of the EU, so that the level of protection after the transfer will not be undermined. Against this argument, there is a counter-argument that, since the law where the data controller locates will also apply to the processing of the personal data of the EU data subjects, it might lead to different results than merely applying the

[203] See SCHANTZ, Peter, Art. 44, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, p. 14, citing KUNER, Christopher, Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law. International Data Privacy Law, 2015, Vol.5, pp. 235-245.
[204] See JUAREZ, Tavares, Art. 44, in: WOLFF; BRINK; v. UNGERN-STERNBERG. BeckOK Data Protection Law (Datenschutzrecht). BeckOK Online-Commentary, 35. Edition, p. 16.
[205] Ibid.
[206] SCHRÖDER, Christian, Art. 44, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 16c.

GDPR.[207] Thus, an extra examination of the legal system of the third country is necessary. If the legal system of the third country cannot provide an equivalent protection to the EU data subjects in comparison to the GDPR, appropriate safeguard must be ensured.

3.3.3 Remained problems

As noted above, both the arguments from the pros and cons side have flaws. More importantly, both positions leave unanswered problems for the practice. The pro-side affirms a data transfer, leading to the question on which legal basis a data transfer can be made, since SCCs and binding corporate rules are designed for the case where there is a controller or processor located within the EU. The con-side denies a data transfer, accordingly, the subsequent disclosure to another party in the third country or another third country does not constitute an onward transfer. It is open for discussion whether this subsequent disclosure could be considered as a (first) data transfer, but at least from a semantic point of view, the data must be transferred from the EU to a third country, i.e. across the EU border, which is not the case in a transfer from a third country controller to another third country controller. However, if no transfer and onward transfer exists, thus no extra obligatory safeguard is needed for the disclosure to parties located in a third country, the question arises how a circumvention of the high level of personal data protection granted by the GDPR can be avoided.

II. Behind the Dispute of Opinions: The Relationship Between Art. 3 (Application Scope) and Chapter V (Data Transfer Rules)

As showed above, the interpretation of the application scope of Chapter V GDPR is highly controversial. This is in particular true in terms of the question, whether the data flow from an EU data processor to a non-EU data controller, and that from an EU data

[207] SCHANTZ, Peter, Art. 44, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, p. 14.

subject to a non-EU data controller, constitutes a data transfer to a third country within the meaning of Chapter V, thus are subject to the restrictions laid down therein.

The wording of Chapter V itself seems to support a wide interpretation of the concept of data transfer, since the GDPR now officially makes the data processor an eligible transferor and imposes compliance obligations on him, which shows an extension of the application scope of the data transfer rules compared to the Data Protection Directive. Nevertheless, the wording of Chapter V is still so general that it leaves some more detailed issues open, for example whether it applies when an EU processor transfers personal data to the non-EU controller that is already subject to the GDPR per Art. 3, whether the transferring (exporting) data controller or processor must be established in the EU, or controllers and processors that are not established in the EU but subject to the GDPR per Art. 3 could also be the transferor, and thus must also bear the same obligation to ensure compliance with the data transfer rules. The answer to these questions cannot be conducted from the wording of Chapter V.

As can be seen above, commentators further tried to interpret Chapter V from a teleological view, namely the function and goal that Chapter V tries to achieve – the level of data protection guaranteed by the GDPR should not be undermined through or after the data transfer.[208] Interestingly, this teleological interpretation is both relied upon by the pro-side and the con-side. Commentators that are against the existence of a data transfer in the aforementioned circumstances argue, since the GDPR applies to the non-EU data controller per Art. 3, the non-EU data controller has to process the data in accordance with the GDPR anyway, thus, there is no risk of undermining the data protection level even if the personal data are sent to a third country.[209] On the contrary, the ones supporting the existence of a data transfer in such circumstances raise concern about whether the direct application of the GDPR per Art. 3 automatically guarantees an adequate level of protection to the transferred personal data in a third country.[210] As demonstrated in chapter 2 of this dissertation, the direct application of the GDPR to data controllers established outside of the EU per Art. 3 is also accompanied by problems. Without trying to make a judgement as whose argument is more persuasive

[208] Recital 101 GDPR.
[209] See above section 3.3.1.
[210] See section 3.3.2.

first, this confrontation of arguments reveals the interactions between Art. 3, regulating the application scope of the GDPR, and the data transfer rules under Chapter V of the GDPR. Both legal institutions involve data flows from the EU to a third country, both serve the same purpose of avoiding circumvention of the stringent EU data protection law,[211] it is not surprising that there are situations where both seem to apply and a delimitation from each other is highly unclear.

The interaction between Art. 3 and Chapter V GDPR was already the object of discussion under the Data Protection Directive. In one of its opinions, the WP 29 has made its position clear that the Safe Harbor, a specific regime for data transfers from the EU to the USA, should not affect the direct application of the Data Protection Directive to the non-EU controllers per Art. 4 (Art. 3 (territorial scope) in the GDPR respectively).[212] Thus, WP 29 held the opinion that the application of the data transfer rules under chapter V does not exclude the application of Art. 3. However, it did not further elaborate the opposite case, namely whether the data transfer rules under Chapter V should still apply when Art. 3 already applies, meaning the non-EU data controller or processor is already subject to the GDPR. After the promulgation of the GDPR, the EDPB has also expressed its willing to "further assess the interplay between the application of the territorial scope of the GDPR as per Art. 3 and the provisions on international data transfers as per Chapter V" and further stated that "additional guidance may be issued in this regard, should this be necessary".[213] Unfortunately, till now, such additional guidance is not yet provided, leaving the issue unsettled and confusing.

Meanwhile, the scholar opinions on the relationship between Art. 3 and Chapter V continue to be controversial and wavering. Some data protection experts once had the opinion that it is not necessary to apply "two sets of overlapping requirements with the same purpose that are not coordinated with each other",[214] and hoped for the data protection reform to clarify this problem. Now, upon the effectiveness of the GDPR, as

[211] KUNER, Christopher, Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law. International Data Privacy Law, 2015, Vol.5, p. 244.
[212] Art. 29 Working Party, Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles", 16 May 2000.
[213] EDPB, Guideline 3/2018 on the territorial scope of the GDPR (Art. 3), version 2.1, 12 November 2019, p. 22.
[214] KUNER, Christopher, Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law. International Data Privacy Law, 2015, Vol.5, p. 244.

things have not gotten any clearer, scholars came to recognize that under the current stand, Art. 3 and Chapter V must be applied separately, and compliance with one does not exclude the obligation to comply with the other.[215]

In the absence of a clear response to this problem by the GDPR, in order to assess whether Art. 3 regulating the direct application scope of the GDPR and Chapter V regulating the transborder data transfers should apply simultaneously to one set of data flow from the EU to a third country, it must be asked whether the application of Art. 3 itself alone is sufficient to ensure an adequate level of protection on the personal data sent to a third country. Since the previous chapter of this dissertation already identified the biggest drawback of a wide application scope of the GDPR per Art. 3, namely the enforcement problem, the answer to the above question probably has to be negative. Against this background, it should be further asked whether the application of Chapter V GDPR, the data transfer rules, could contribute to solve the enforcement problem and establish a better protection of personal data of EU data subjects in third countries, without impeding the international data flow disproportionally. Bearing this question in mind, the following chapter will look into the conditions and legal bases required for data transfer to a third country laid down in Chapter V GDPR, in order to investigate whether the application of the data transfer rules provides a more enforceable protection to the data subjects with regard to their personal data, when they are processed by a third-country data controller.

III. Data Transfers from the EU to a Third Country or International Organization

Chapter V GDPR plays a crucial role for regulating data flows from the EU to a third country or international organization, by imposing certain conditions on the data flows that are identified as data transfers to a third country or international organization. Only if these conditions are met, a data transfer to a third country or international organization is allowed. This is usually referred to as the principle of "prohibition with

[215] KUNER, Christopher, Art. 44, in: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher, The EU Data Protection Regulation (GDPR): A Commentary. Oxford University Press, Oxford, 2020, p. 1153; see also SCHRÖDER, Christian, Art. 44, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 16a.

reservation of permission" in the literature.[216] Art. 44 stipulating the general principles for data transfers imposes two prerequisites for transferring personal data to a third country or international organization. First, a data transfer is subject to the other provisions of the GDPR, for example the transfer as a type of processing has to meet the general principles of data processing, including having a legal basis according to Art. 6 GDPR; second, the conditions laid down in Chapter V, which are specifically aimed at regulating data transfers to a third country or international organization, must be complied with by the controller or processor. Since this dissertation focus on the third country, not on the international organizations, in the following data transfers to international organization will be left out for the purpose of conciseness.

The conditions (also legal bases) for the data transfers are provided in Chapter V. There are generally three of them: First, personal data may be transferred to a third country if the Commission has decided that the third country as a whole or some of its specific sectors ensure an adequate level of protection for personal data ("adequacy decision"), second, in the lack of such adequacy decision, personal data may be transferred to a third country if the controller or processor provides appropriate safeguards, third, in the absence of a adequacy decision and appropriate safeguards, personal data may be transferred to a third country upon the derogations for specific situations.[217]

It has to be noted that when applying these conditions/legal bases, a certain hierarchy must be followed. As indicted by their names, whereas adequacy decisions and appropriate safeguards aim to ensure that the personal data transferred to a third country will continue to enjoy high level protection in that third country,[218] the derogations are exceptions from the high level protection which provide neither guarantee nor safeguard on the personal data transferred to a third country, meaning the transferred personal data will be processed according to the law of the third country at the discretion of the recipient.[219] Due to this difference, and the general goal of the data transfer rules to prevent the level of protection guaranteed by the GDPR being undermined in the third country, Art. 29 Working Party has held that the data controller or processor should

[216] PAULY, Daniel A, Art. 44, in: PAAL, Boris P.; PAULY, Daniel A, GDPR German Data Protection Act (DS-GVO BDSG), C.H.BECK, 3rd Edition 2021, p. 1.
[217] Art. 45, 46 and 49 GDPR.
[218] Art. 29 Working Party, Working document on a common interpretation of Art. 26 (1) of Directive 95/46/EC of 24 October 1995, 25 November 2005, p. 6.
[219] Ibid.

favor solutions that allow the EU data subjects to continue benefiting from the fundamental rights and safeguards conferred to them by the GDPR.[220] More specifically, this means, according to the suggestions of the Art. 29 Working Party, a data controller or processor should first consider whether the third country involved provides an adequate level of protection. If not, the controller or processor should consider to transfer the personal data based on appropriate safeguards. Only if this is truly infeasible or even impossible, should the data controller or processor consider to use derogations.[221] In other words, since derogations are not in the position to provide any extra protection to the personal data transferred to a third country, it should not be a first choice or generally relied upon to transfer personal data from the EU to a third country. In addition, the application conditions of the derogations must be interpreted restrictively.

In the following, the specific application requirements and features for each alternative will be analyzed, with a focus on the enforcement possibilities.

1. Adequacy decision

The easiest and securest way for a data controller or processor to transfer personal data from the EU to a third country is to base the transfer on an existing adequacy decision, which is issued by the Commission on that third country or a specific sector of that country. In this case, the data controller or processor involved does not need to take any extra steps or measures to safeguard the data transferred, since the involved third country already provides an equivalent level of protection compared to that is guaranteed in the EU.

With this strong and comprehensive legal effect as result, not surprisingly, the assessment of adequacy is subject to very strict criteria. These criteria can be primarily found in Art. 45 section 2 GDPR, which serves as a primary legal source for the assessment of the data protection level in a third country. Except for that, there is no definition of "adequate level of protection" can be found in the GDPR. The CJEU has

[220] Ibid, p. 8.
[221] Ibid, p. 9.

interpreted in "Schrems I"[222] concerning the validity of the EU-US "Safe Harbour" that an adequate level of protection should be understood as requiring the third country in question provides a level of protection of fundamental rights and freedoms that is "essentially equivalent" to that is guaranteed within the EU.[223] However, what the legal system of the third country has to offer, in order to be assessed as providing a level of protection that is "essentially equivalent" to that guaranteed in the EU, is somewhat still vague. In that regard, a more specific guidance was provided by the Art. 29 Working Party in one of its opinions in 2017 that was later endorsed by the EDPB ("Opinion on Adequacy Decision").[224] It is made clear in this Opinion on Adequacy Decision that, when making an adequacy assessment, the Commission needs to consider not only the content of data protection rules in the third country in question, but also the enforcement system of that country that ensures the effective functioning of those rules in the practice, especially the administrative and judicial redress systems.[225] Besides, the legal framework of access of public authorities to personal data in the course of criminal law enforcement or national security must also be considered.[226] Based on this, the Art. 29 Working Party has identified an array of specific elements that shall be considered in any adequacy assessment.

1.1 Core contents of the data protection material rules

Pursuant to the Opinion on Adequacy Decision, a third country's data protection law system must contain the following content principles:[227]

- Basic data protection copes and principles
- Grounds for lawful and fair processing for legitimate purposes
- The purpose limitation principle

[222] Case C-362/14, 06.10.2015.
[223] CJEU, C-362/14, 06.10.2015, para. 73.
[224] Art. 29 Working Party, Adequacy Referential (updated), adopted on 28 November 2017 and endorsed by the EDPB on 25 May 2018.
[225] Art. 29 Working Party, Adequacy Referential (updated), p. 3.
[226] Ibid, p. 4.
[227] Ibid, p. 5-6.

- The data quality and proportionality principle
- Data retention principle
- The security and confidentiality principle
- The transparency principle
- The right of the data subjects of access, rectification, erasure and objection
- Restrictions on onward transfers

If a third country's legal system is to be assessed as providing a level of protection essentially equivalent to that of the EU, these substantial data protection rules must exist in the legal system of the third country. Except for these core principles, there are also additional requirements for specific type of processing operations, for example, the processing of special categories of personal data, processing for the purpose of direct marketing and automated decision making and profiling.[228]

1.2 Enforcement mechanism

In addition to the substantial data protection rules, the legal system in the third country must provide practical and effective enforcement possibilities, to make sure that the substantial rules mentioned above are indeed complied with in the practice, and the data subjects have effective means to exercise their rights. In this regard, the Opinion on Adequacy Decision lists four elements that should exist in the third country to ensure an effective enforcement mechanism from the EU point of view:[229]

- One or more competent independent supervisory authority
- A good level of compliance
- Accountability of the data controller

[228] Ibid, p. 7.
[229] Ibid, p. 8.

- Support provided by the legal system to the data subjects in the exercise of their rights and appropriate redress mechanisms

1.3 Rules concerning data access by public authorities for law enforcement and national security purposes

Another issue addressed by the CJEU in "Schrems I"[230] and in "Schrems II"[231] is the access of personal data by public authorities for law enforcement and national security purposes. In "Schrems I", the CJEU invalidated the EU-US Safe Harbor with mainly two arguments. First, the Safe Harbor principles are not binding to the data access by the public authorities.[232] The CJEU has also ascertained that, under the framework of the Safe Harbor, data access by the public authorities for purposes of "national security, public interest, or law enforcement" rather has primacy over the fundamental rights of the data subjects whose personal data are transferred from the EU to the US, and the Commission did not provide further information regarding to whether and what kinds of limitations the US legal system has put on the data access by public authorities.[233] Second, the CJEU noted that the Safe Harbor Decision did not examine whether there are effective legal remedies in the US against the data access by the public authorities.[234] Further, in "Schrems II", the CJEU announced the "Privacy Shield", negotiated by the EU and the US after the invalidation of the Safe Harbor, invalid too. The CJEU noted that the Privacy Shield Decision, as regards the data access by public authorities arising from some of the surveillance programs in the US, expressly the ones that are based on Section 702 of the FISA and on E.O. 12333, do not ensure a level of protection essentially equivalent to that is guaranteed within the EU.[235] That is because, first, the data access by public authorities under those surveillance programs as an interference of the fundamental rights of the EU data subject does not respect the essence of those fundamental rights and fail to satisfy the principle of proportionality,[236] and second, the data subjects are not granted with enforceable rights against the public

[230] CJEU, C-362/14, 06.10.2015.
[231] CJEU, C-311/18, 16.07.2020.
[232] CJEU, C-362/14, 06.10.2015, para. 82.
[233] Ibid, para. 86, 87.
[234] Ibid, para. 89.
[235] CJEU, C-311/18, 16.07.2020, para. 185.
[236] Ibid, para. 179-185.

authorities before the court, especially no right to an effective judicial remedy.[237] The latter cannot be made up even if there is a Ombudsperson under the framework of the Privacy Shield, who acts as a "Senior Coordinator for International Information Technology Diplomacy", since the Ombudsperson is not independent from the executive and its decision is not binding on the intelligence services.[238]

Besides, taking into consideration of the requirements imposed by the CJEU in "Schrems I" and in order to further clarify the requirements set for interferences with the fundamental rights to privacy and data protection through surveillance measures, the WP 29 has issued an opinion providing that the third country's legal system should meet four requirements, which are called by the WP29 as the "European Essential Guarantees":[239]

- Processing should be based on clear, precise and accessible rules
- Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated
- An independent oversight mechanism should exist
- Effective remedies need to be available to the individual

Together, the case-law of the CJEU and the opinions of the WP 29 have framed the threshold for assessing whether the data access by public authorities in the third country for purposes of national security, public interest, or law enforcement (including surveillance programs on such grounds) is proportionate and ensures a level of protection essentially equivalent to that guaranteed within the EU. These factors must be borne in mind when making an adequacy assessment with regard to any other country.

To sum up, the level of protection provided by the legal system of a third country to data subjects must be assessed in the light of the above elements and standards. Meanwhile, the adequacy decision may not only refer to a third country as a whole, it

[237] Ibid, para. 186-197.
[238] Ibid, para. 193-196.
[239] Art. 29 Working Party, working document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 13 April 2016, p. 6.

can also be limited to a specific sector, for example, the adequacy decision on Japan only applies to the processing of personal data by business operators, not those by public authorities.[240]

2. General about the appropriate safeguards

In the absence of an adequacy decision, a data controller or processor may only transfer personal data to a third country subject to the existence of appropriate safeguards. Since there are only 12 countries that have received an adequacy decision from the European Commission for the moment, data transfers from the EU to most countries have to base on the appropriate safeguards.

2.1 Accountability of the parties involved in the transfer

Compared to the adequacy approach, the appropriate safeguards are considered by some scholars and policy advisors as manifestations of the "organizationally-based approach" for data transfers.[241] This "organizationally-based approach" is also called the "accountability approach".[242] Departing from the location of the data or the general data protection level of the importing country, the accountability approach focuses more on the responsibilities of the involved organizations, i.e. the data transferring parties.[243] It requires the data controllers or processors who export the personal data to a third country to remain accountable for the data wherever such data are transferred or processed.[244] To that end, the parties involved in the data transfer must adopt inter-party, contractual measures to create an private law relationship,[245] by which the

[240] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, para. 4.
[241] KUNER, Christopher, Transborder Data Flows and Data Privacy Law. Oxford University Press, Oxford, 2013, p. 71; Centre for Information Policy Leadership White Paper, Essential Legislative Approaches for Enabling Cross-border Data Transfers in a Global Economy, 25 September 2017.
[242] Ibid.
[243] BENNETT, Colin; ODURO-MARFO, Smith, Global Privacy Protection: Adequate Laws, Accountable Organizations and/or Data Localization? Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers, 2018, p. 881.
[244] Ibid.
[245] SCHRÖDER, Christian, Art. 46, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 10.

importing party in the third country obliges itself to process the personal data in accordance with the EU data protection law.

2.2 Enforceable data subject rights

Through the appropriate safeguards, data subjects in the EU should be able to continue enjoying and effectively exercising the rights laid down in Chapter III GDPR, after their personal data are transferred outside of the EU. This is particularly important since the data importer in the third country is not necessarily subject to the GDPR, and even if it is subject to the GDPR, Chapter 2 of this dissertation has come to the conclusion that the enforcement of the rights of data subjects against a data controller or processor located in a third country faces significant difficulties. This problem should be addressed when applying the appropriate safeguards.

From the available appropriate safeguards listed in Art. 46, in particular the SCCs and the requirements imposed on the binding corporate rules, it can be observed that, first, any appropriate safeguard must grant data subjects the same material rights conferred to them in the GDPR. Second, the enforceability of the data subject rights should be enhanced by the self-commitment of the data importer in the third country to allow the data subjects to exercise their rights.[246] This commitment is to a large extent made by means of contract with third-party beneficial provisions.[247] More specifically, in the case of SCCs, the data importer in the third country reaches an agreement with the data exporter in the EU, in the case of corporate binding rules with the other members of the corporate and in the case of code of conducts with the association.[248] In all these contractual relationships, the data subject as a third party should be granted an array of rights that can be exercised against the data importer in the third country and/or the data exporter in the EU.

[246] SCHANTZ, Peter, Art. 46, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, p. 8.
[247] Ibid.
[248] Ibid.

2.3 Effective legal remedy for data subjects

Appropriate safeguards should also be able to provide data subjects with effective legal remedy options. Art. 46 does not elaborate in which jurisdiction the data subjects are to be granted effective legal remedies, whether in the EU or in the third country to which the personal data is transferred. It can be seen from the SCCs adopted by the European Commission so far that the data importer in the third country may in any case subject itself to the jurisdiction of a Member State of the EU by adopting a "choice of forum" clause in the contractual safeguards, so that the data subject could seek legal remedies in a EU Member State.

It is unclear whether a legal remedy will be deemed effective and enforceable, if the EU data subjects are only provided with the possibility to seek for legal remedy in a third country. The wording of recital 108 seems to favor an answer in the positive, since it says that "…effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country", therefore, it should be sufficient if the data subjects are granted legal remedies in a third country.[249] However, from a practical point of view, the data subjects have factual difficulties to seek for legal remedies in a third country due to the intensive costs and lack of resources.

2.4 Type of the appropriate safeguards and respective conditions

The appropriate safeguards available for transferring personal data to a third country are listed non-exclusively in Art. 46 GDPR. Beyond this, the parties may also adopt other extra measures to provide adequate safeguards on the protection of personal data in a third country. Art. 46 section 2 stipulates 5 alternatives that can provide appropriate safeguards for data transfers to a third country, without having to be authorized by a supervisory authority. Given the scope and focus of this dissertation, only 4 of them are relevant to the data transfers dealt with in this dissertation, thus, the following part will not refer to the safeguard provided for data transfers between public authorities. Other

[249] See also LANGE; FILIP, Art. 46, in: WOLFF; BRINK; v. UNGERN-STERNBERG, BeckOK Data Protection Law (Datenschutzrecht). BeckOK Online-Commentary, 35. Edition, p. 10.

alternatives will be introduced in details below.

2.4.1 Standard data protection clauses

Standard data protection clauses, also called SCCs ("SCCs") are adopted by the European Commission or drafted by a supervisory authority and then approved by the Commission.[250] After the adoption of the Commission Decision 2021/914 on the standard contractual clauses on 4 June 2021,[251] there are four sets of SCCs applicable to four different modules: module 1 "controller to controller", module 2 "controller to processor", module 3 "processor to processor" and module 4 "processor to controller", which should replace the three sets of effective SCCs that were issued under the Data Protection Directive ("New SCCs").

As indicated by its name, SCCs are typical contractual mechanism adopted between two parties with equal legal status. It may be concluded separately or incorporated in a contract between the data exporter and the data importer, which simultaneously governs other business-related issues.[252] In order to be full effective, SCCs issued by the Commission must be invoked by the parties without alteration, so that the data transfer based thereof will no longer have to be authorized by a supervisory authority. Any alteration of the SCCs will lead to the clauses being no more "standard" and must be authorized by the competent supervisory authority according to Art. 46 section 3. Notwithstanding, as noted above, SCCs may be supplemented by other clauses. If such supplementary measures are in place, they must not in any way contradict to the SCCs or changes the content of the SCCs,[253] in any case not at the expense of data subjects.

---

[250] Art. 46 section 2 (c) and (d) GDPR.
[251] Commission Implementing Decision (EU) 2021/914 of June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, 4 June 2021.
[252] Ibid, recital 3.
[253] Same opinion PAULY, Daniel A, Art. 46, in: PAAL, Boris P.; PAULY, Daniel A, GDPR German Data Protection Act (DS-GVO BDSG), C.H.BECK, 3rd Edition 2021, p. 21; alterations allowed for the favor of the data subject see SCHANTZ, Peter, Art. 46, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, p. 32; LANGE; FILIP, Art. 46, in: WOLFF; BRINK; v. UNGERN-STERNBERG, BeckOK Data Protection Law (Datenschutzrecht). BeckOK Online-Commentary, 35. Edition, p. 29; GABEL, Detlev, German Data Protection Act old version (BDSG aF) § 4 c, in: TAEGER, Jürgen; GABEL, Detlev. GDPR-German Data Protection Act (DSGVO-BDSG). Specialist Media Law and Economics, 3rd Edition 2019, p. 27.

2.4.2 Binding corporate rules

Binding corporate rules approved by the competent supervisory authority also serve as a legal basis for transferring personal data from the EU to a third country. As a legal concept defined in Art. 4 (20) of the GDPR, binding corporate rules are referred to as personal data protection policies adopted by data controller(s) or processor(s) established within the EU and data controller (s) or processor (s) established outside of the EU but within a group of undertakings or group of enterprises engaged in a joint economic activity, usually for the purpose of transferring personal data from the EU to a third country.[254] In this regard, a "group of undertakings" means "a controlling undertaking and its controlled undertakings",[255] i.e. the parent company and its dependent subsidiaries. On the contrary, a "group of enterprises engaged in a joint economic activity" is a group of companies that do not stay in a controlling-and-controlled relationship to each other, but are economically strongly linked to each other.[256] A important example arising from the EU-China business practices is a joint venture grounded by a European company and a Chinese company in China according to the Chinese Foreign Investment law.[257] In this case, the European company, the Chinese company and the joint venture could be deemed as a group of companies that pursue the same economic activities. Nevertheless, as many scholars have correctly pointed out, while the threshold for identifying a group of enterprises engaging in a joint economic activity might not be high, the material requirements laid down in Art. 47 GDPR for an approvable binding corporate rules, such as, the liability delegation, are not likely to be fulfilled by companies that are not connected to each other closely enough.[258] Thus, although the GDPR extends the application scope of binding

---

[254] Art. 4 section (20) GDPR.
[255] Art. 4 section (19) GDPR.
[256] SCHRÖDER, Christian, Art. 46, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 13; SCHRÖDER, Christian, Art. 47, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 13.
[257] Opinions for joint ventures see TOWFIGH, Emanuel V.; ULRICH, Jacob, Art. 4, in: SYDOW, Gernot. EU GDPR (Europäische Datenschutzgrundverordnung). Nomos, 2nd Edition 2018, p. 226; ZERDICK, Thomas, Art. 47, in: EHMANN, Eugen; SELMAYR, Martin, General Data Protection Regulation (Datenschutz-Grundverordnung). C.H.BECK, 2nd Edition 2018, p. 8; Sceptical about joint ventures SCHRÖDER, Christian, Art. 47, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 13.
[258] SCHRÖDER, Christian, Art. 47, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 13; GABEL, Detlev, Art. 47, in: TAEGER, Jürgen;

corporate rules to a group of enterprises engaged in a joint economic activity, the use of it will still be very much limited, in particular compared to the SCCs mentioned above.

The minimum content of the binding corporate rules is specified in Art. 47 GDPR. In addition to the basic information regarding the concerned group members and the data transfers, the binding corporate rules must in particular specify the binding nature of the binding corporate rules both internally and externally, the application of the data processing principles and rights of the data subjects as guaranteed in the GDPR, the liability allocation, and the implementation and supervision mechanism. Thus, the material rules concerning the data processing and the rights of the natural persons in the GDPR are repeated in the binding corporate rules. Moreover, effective implementation and supervision measures are required to ensure that these material rules will be complied with in the corporate practice.

As regard to the enforcement of the data subject rights and legal remedies, first, the means to exercise data subject rights must be explicitly provided in the binding corporate rules.[259] Second, if damages occur due to the infringement of the data subject rights, the data controller or processor established within the EU must assume liability for any breach of the binding corporate rules by any member established outside of the EU.[260] Through this contractually agreed joint liability between the members of the group, costs intensive legal proceedings against third-country data importers can be avoided, data subjects are provided with a practically feasible, effective option to enforce their rights.

2.4.3 Codes of conduct

Appropriate safeguards may also be provided by an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third

GABEL, Detlev, GDPR-German Data Protection Act (DSGVO-BDSG). Specialist Media Law and Economics, 3rd Edition 2019, p. 2; PAULY, Daniel A, Art. 47, in: PAAL, Boris P.; PAULY, Daniel A, GDPR German Data Protection Act (DS-GVO BDSG), C.H.BECK, 3rd Edition 2021, p.4.

[259] Art. 47 section 2 (e) GDPR.

[260] Art. 47 section 2 (f) GDPR.

country to apply the code of conduct, including as regards data subject rights.[261] In that regard, Art. 40 section 3 GDPR specifically provides that in addition to controllers or processors subject to the GDPR, controllers or processors not subject to the GDPR may also adhere to codes of conduct that are approved by the competent supervisory authority and affirmed to have general validity within the EU by the Commission,[262] in order to provide justification for data transfers from the EU to a third country. An additional requirement is that the aforementioned controllers or processors must make binding and enforceable commitments, via contractual or other legally binding instruments, to apply the adhered code of conduct including with regard to the rights of data subjects.[263] Therefore, in general, scholars have summarized three prerequisites that must be fulfilled in order to transfer personal data from the EU to a third country based on codes of conduct: a code of conduct approved by the competent supervisory authority and decided by the Commission as having general validity within the EU, a binding commitment of the data controller or processor in the third country to apply the code of conduct, and effective enforceability possibilities including as regards the data subject rights.[264]

2.4.3.1 The content and approval of codes of conduct

A code of conduct can be drafted by an association or other body representing a category of data controllers or processors.[265] The draft is then to be submitted to the competent supervisory authority for approval. If the submitted code of conduct concerns processing activities in several Member States, the competent supervisory authority must submit it to the EDPB.[266] The EDPB shall provide an opinion on whether the code of conduct complies with the GDPR or provides appropriate safeguards. In the case of a positive assessment, the EDPB shall submit its opinion to the Commission and the Commission may then decide that the code of conduct has

[261] Art. 46 section 2 (e) GDPR.
[262] Art. 40 section 3 GDPR.
[263] Ibid.
[264] See PAULY, Daniel A, Art. 46, in: PAAL, Boris P.; PAULY, Daniel A, GDPR German Data Protection Act (DS-GVO BDSG), C.H.BECK, 3rd Edition 2021, pp. 34-36; ROSSNAGEL, Alexander, Art. 40, in: SIMITS, S.; HORNUNG, G.; SPIECKER gen. DÖHMANN, I, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, p. 51.
[265] Art. 40 section 1 GDPR.
[266] Art. 40 section 7 GDPR.

general validity within the EU.[267]

Further, if the purpose of using a code of conduct is to provide adequate safeguards on data transfers to a third country, the material content of such a code of conduct must contain all the essential rules and mechanisms of the GDPR that are required for ensuring an appropriate level of fundamental right protection in a third country,[268] such as the data processing principles, the rights of the data subjects and the various obligations of the data controllers or processors.

2.4.3.2 Binding commitment of the controllers or processors in the third country to apply the code of conduct

Although a code of conduct is drafted by an association representing a category of data controllers or processors and approved by the competent supervisory authority, it has no automatic binding effect to the data controllers or processors in the concerned sector, in the absence of a contractual or statutory legal basis.[269] A contractual or quasi-contractual binding effect may come into being, if for example the Articles of Association imposes an obligation on the members of the association to apply the approved code of conduct, or a data controller or processor voluntarily obliges itself to apply the code of conduct.[270] In this sense, data controllers or processors that are not members of the association can also subject itself to the code of conduct.[271]

---

[267] Art. 40 section 9 GDPR.

[268] Ibid; SCHANTZ, Peter, Art. 46, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, p. 67.

[269] BERGT, Matthias; PESCH, Paulina Jo, Art. 40, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 8; WOLFF, Heinrich Amadeus, VI. International Data Traffic with Countries Outside the Union (Internationaler Datenverkehr mit Staaten außerhalb der Union), in: SCHANTZ, Peter; WOLFF, Heinrich Amadeus, The New Data Protection Law (Das neu Datenschutzrecht), C.H.BECK, 1st edition 2017, p. 1285.

[270] BERGT, Matthias; PESCH, Paulina Jo, Art. 40, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 8; JUNGKIND, Art. 40, in: WOLFF, Heinrich Amadeus; BRINK, Stefan; UNGERN-STERNBERG, Antje v., BeckOK Data Protection Law (Datenschutzrecht). BeckOK Online-Commentary, 35. Edition, p. 26; LEPPERHOFF, Niels, Arts. 40 and 41, in: GOLA, Peter; HECKMANN, Dirk, Commentary on the GDPR (DS-GVO), C.H. BECK, 2nd edition 2018, p. 22; PAULY, Daniel A; KUMKAR, Lea Katharina, Art. 40, in: PAAL, Boris P.; PAULY, Daniel A, GDPR German Data Protection Act (DS-GVO BDSG), C.H.BECK, 3rd Edition 2021, p. 9a; SCHWEINOCH, Martin, Art. 40, in: in: EHMANN, Eugen; SELMAYR, Martin, General Data Protection Regulation (Datenschutz-Grundverordnung). C.H.BECK, 2nd Edition 2018, p. 52; WOLFF, Heinrich Amadeus, VI. International Data Traffic with Countries Outside the Union (Internationaler Datenverkehr mit Staaten außerhalb der Union), in: SCHANTZ, Peter; WOLFF, Heinrich Amadeus, The New Data Protection Law (Das neu Datenschutzrecht), C.H.BECK, 1st Edition 2017, p. 1285.

[271] BERGT, Matthias, Rules of Conduct as a Means of Eliminating Legal Uncertainty in the General Data Protection

This binding effect of the code of conduct is required for the purpose of providing appropriate safeguards for data transfers to a third country. As stipulated in Art. 46 section 2 (e) and Art. 40 section 3, in order to justify data transfers to a third country, the controller or processor in the third country must make a binding commitment to apply the approved and general valid code of conduct. The above-mentioned two provisions do not specify how such binding commitment can be made, Art. 40 section 3 only gives an example of "via contractual or other legally binding instruments".

As demonstrated above, in the absence of further clarity provided by the guidelines of the EDPB or from the data protection supervisory authorities, theoretically, this binding commitment may be made by various ways, dependent on the rules of the association that has drafted the code of conduct. For example, a data controller or processor in the third country may become a member of the association, thereby be obligated to apply the code of conduct as required by the Articles of Association (if such requirement exists in the Articles of Association), or conclude a contract with the association which obliges the data controller or processor to apply the code of conduct,[272] or otherwise creates a unilateral binding obligation to apply the code of conduct for itself.[273] In any case, it should lead to the result that the data controller or processor in the third country is bindingly obligated to apply the code of conduct.

The subjection of the data controller or processor to the code of conduct means that the data controller or processor is at the same time subject to the monitoring of the monitoring body, since it is mandatory for the code of conduct to contain such monitoring mechanism.[274] This monitoring body is accredited for the purpose of monitoring the compliance with the code of conduct by the competent supervisory authority.[275] The code of conduct should grant the monitoring body with appropriate competences and powers to monitor the compliance with the code of conduct by the

Regulation (Verhaltensregeln als Mittel zur Beseitigung der Rechtsunsicherheit in der Datenschutz-Grundverordnung). Computer und Recht, 2016, Vol.32, No. 10, p. 673.

[272] LAUE, Philip, § 8 Self-regulation (Selbstregulierung), in: LAUE, Philip; KREMER, Sascha, The New Data Protection Law in Business Practice (Das Neue Datenschutzrecht in der Betrieblichen Praxis), 2nd edition 2019, p. 9; PAULY, Daniel A; KUMKAR, Lea Katharina, Art. 40, in: PAAL, Boris P.; PAULY, Daniel A, GDPR German Data Protection Act (DS-GVO BDSG), C.H.BECK, 3rd Edition 2021, p. 9a.;
[273] See SCHANTZ, Peter, Art. 46, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, p. 68.
[274] Art. 40 section 4 GDPR.
[275] Art. 41 section 1 GDPR.

data controller or processor that is bindingly subject to it. For example, the power to impose a sanction in the event of non-compliance, which includes from issuing a warning to ordering a contractual penalty till suspension or exclusion of the concerned controller or processor from the code.[276]

Such competences and powers of the monitoring body is rather contractual,[277] since it is agreed to by the data controller or processor when it subjects itself to the code of conduct according to the Articles of Association or by another contractual or unilateral means.

2.4.3.3 Enforceability for the data subject as regards the data subject's rights

That the data subject must be granted with enforceable data subject rights and effective legal remedies is a general requirement for the appropriate safeguards laid down in Art. 46 section 1. Specifically, with regard to the code of conduct as a type of appropriate safeguard, Art. 46 section 2 (e) and Art. 40 section 3 both stipulate that the commitment of the data controller or processor in the third country to apply the appropriate safeguards should be enforceable, including as regards data subject's rights. Therefore, in addition to the subjection to the code of conduct and its monitoring mechanism discussed above, the commitment of the data controller or processor in the third country must also enable the data subject to exercise and enforce the data subject's rights.[278] This commitment in favor of the data subject can be made together with the aforementioned binding commitment to apply the code of conduct, likewise through a contract with third-party beneficial clauses,[279] or if the data controller or processor has a direct contractual relationship with the data subject, it can also be provided directly

[276]ROSSNAGEL, Alexander, Art. 40, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, p. 54; BERGT, Matthias; PESCH, Paulina Jo, Art. 40, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 22.

[277] See also LEPPERHOFF, Niels, Arts. 40 and 41, in: GOLA, Peter; HECKMANN, Dirk, Commentary on the GDPR - Federal Data Protection Law (DS-GVO/BDSG), C.H. BECK, 2nd Edition 2018, p. 9.

[278] See also SCHWEINOCH, Martin, Art. 40, in: EHMANN, Eugen and SELMAYR, Martin, General Data Protection Regulation (Datenschutz-Grundverordnung), C.H. BECK, 2nd edition, 2018, p. 38; ROSSNAGEL, Alexander, Art. 40, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, p. 51.

[279] BERGT, Matthias; PESCH, Paulina Jo, Art. 40, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 9; SCHWEINOCH, Martin, Art. 40, in: EHMANN, Eugen and SELMAYR, Martin, General Data Protection Regulation (Datenschutz-Grundverordnung), C.H. BECK, 2nd Edition, 2018, p. 38.

in such contractual relationship, for example by applying the general terms and conditions of the data controller or processor which contains the commitment to the data subject.[280] This helps to provide the data subject with a contractual legal basis to exercise its rights and seek for legal remedies against the data controller or processor established in the third country.

2.4.4 Data protection certification

Another legal basis pursuant to Art. 46 section 2 (f) for data transfers to a third country, is an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights. In parallel with the codes of conduct, the conditions for data transfers to a third country based on this appropriate safeguard must be met. This includes, the existence of an approved certification mechanism, the certification of the processing operations carried out by the controller or processor in the third country, and the binding and enforcement commitment of the data controller or processor in the third country to apply the appropriate safeguards, including the enforceable rights and effective legal remedies of the data subjects.[281]

2.4.4.1 Certification by an accredited certification body pursuant to an approved certification mechanism

According to Art. 42 section 5, the competent body to issue a data protection certification is either a certification body accredited by the competent supervisory authority or the national accreditation body, or the competent supervisory authority itself. The certification is to be issued based on the criteria approved by the competent authority or the EDPB in the consistency mechanism. How and by whom these criteria are to be drafted, is not clarified in the relevant provisions. It is reasonable to assume

[280] BERGT, Matthias; PESCH, Paulina Jo, Art. 40, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 9.
[281] SCHANTZ, Peter, Art. 42, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, p. 27-29.

that the accredited certification body or the competent supervisory authority that intend to carry out certification activities may draft the criteria itself, and then submit to the competent authority for approval.[282] Compared to the code of conduct, the explicit requirement of a Commission decision to provide the data protection certification mechanism with general validity within the EU is absent, even if it aims to provide appropriate safeguards for data transfer to a third country. However, some scholars have argued that with regard to certification mechanisms intended to provide legal basis for data transfer to a third country, the certification criteria must be submitted to the EDPB for opinion within the framework of the consistency mechanism.[283] Some other scholars hold that the certification criteria approved alone by the competent authority could also justify data transfer to a third country.[284] This issue is thus still controversial and should be clarified in the future.

Should a certification mechanism be used to provide legal basis for data transfer to a third country, this function must be explicitly aimed by the certification body, and the certification criteria must take into consideration the high requirements imposed on the appropriate safeguards.[285] The certification mechanism should also contain a procedure to regularly review whether the requirements for the certification are still met after the certification. If the requirements for the certification are no longer met, the certification body must withdraw the certification according to Art. 42 section 7 GDPR. In addition to this, it is not specified in the GDPR whether the certification body may have the competence and power to impose any sanctions in case the processing operations of the data controller or processor in the third country do not comply with the certification criteria. However, it is not excluded that such competence and power may be agreed between the data controller or processor in the third country and the certification body.

---

[282] SCHANTZ, Peter, Art. 42, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st edition, 2019, p. 38; BERGT, Matthias; PESCH, Paulina Jo, Art. 42, in: KÜHLING, Jürgen; BUCHNER, Benedikt. GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 16.

[283] SCHANTZ, Peter, Art. 42, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition, 2019, p. 39; WILL, Art. 42, in: EHMANN, Eugen and SELMAYR, Martin, General Data Protection Regulation (Datenschutz-Grundverordnung). C.H. BECK, 2nd Edition 2018, p. 35.

[284] See BERGT, Matthias; PESCH, Paulina Jo, Art. 42, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR (DS-GVO), C.H. BECK, 3rd Edition 2020, p. 30.

[285] SCHANTZ, Peter, Art. 42, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition, 2019, p. 27.

2.4.4.2 Binding and enforceable commitments of the data controller or processor to apply the appropriate safeguards

Same as in the case of code of conduct, data controllers or processors in the third country have to make binding and enforceable commitments to apply the appropriate safeguards, also as regards the data subjects' right. The GDPR does not specify how and to whom these binding and enforceable commitments shall be made. According to scholarly opinions, such commitments may be made by self-binding unilateral announcement,[286] in a contract with third party (data subjects) beneficial clauses or in the General Terms and Conditions of the data controller or processor in the third country.[287] In any case, such commitments should be enforceable by the data subjects, since Art. 46 generally requires that enforceable data subject rights and effective legal remedies should be available for the data subject.

2.5 High requirements on appropriate safeguards after "Schrems II"

2.5.1 The "Schrems II" judgement concerning the SCCs

What the appropriates safeguards together with enforceable data subject rights and effective legal remedies mean in the practice, cannot be directly extracted from the GDPR. Regarding this question, it is the CJEU's opinion in "Schrems II" that, the appropriates safeguards, enforceable data subject's rights and effective legal remedies mean that the personal data transferred to a third country are afforded a level of protection that is essentially equivalent to that guaranteed within the EU.[288] In dealing with another question referred to the CJEU by the referring court, namely whether the SCCs Decision of the Commission ensures an adequate level of protection, the CJEU held that the SCCs contained in the SCC Decision are not invalid merely because they are not binding to the public authorities in the third country where the personal data are

[286] SCHANTZ, Peter, Art. 46, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition, 2019, p. 74.
[287] See BERGT, Matthias; PESCH, Paulina Jo, Art. 42, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR (DS-GVO), C.H. BECK, 3rd Edition 2020, p. 29.
[288] CJEU, C-311/18, 16.07.2020, para. 105.

transferred to, given the contractual nature of these clauses.[289] However, the validity of the SCCs does not automatically imply that the personal data transferred to the third country are afforded a level of protection essentially equivalent to that is guaranteed within the EU. The CJEU made it clear that, the SCCs only intend to provide contractual guarantees between the transferring parties, they are not capable to ensure an adequate level of protection in all cases universally.[290] Where the standard contractual clause are not able to ensure an adequate level of protection to the personal data transferred, because the law of the third country contains rules that might impinge the guarantees contained in the contractual means, the controller or processor need to adopt supplementary measures.[291] To that end, the controller or processor in the EU needs to assess, together with the recipient in the third country, on a case-by-case basis, whether the law of the third country indeed contains rules that might impinge the contractual guarantee provided by the standard data protection clauses, if yes, whether and what kind of supplementary measures can be taken to compensate that deficiency. If, after the assessment, the controller or processor comes to the conclusion that no additional supplementary measures can be taken to ensure an adequate level of protection, the controller or processor must suspend or end the data transfer. If he or she fails to do that, the competent supervisory authority should order the suspension of the data transfer.[292]

The above illustrated ruling of the CJEU in "Schrems II" pose new challenges on the data transfer parties. First, it basically requires the data controller or processor to make an "mini adequacy decision", as regards whether the legal system of the third country could impinge on the effectiveness of the standard data protection clauses.[293] This requires first, that the data controller or processor in the EU as data exporter, with the help of the data recipient in the third country, has a comprehensive understanding of the legal system of the third country where the personal data are transferred to. In addition, the factors or standards that must be taken into consideration in such assessment are not straightforward. In this regard, the CJEU merely mentioned the data access by public

[289] Ibid, para. 136.
[290] Ibid, para. 133.
[291] Ibid.
[292] Ibid, para. 135.
[293] SCHRÖDER, Christian, Art. 46, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 17a.

authorities of the third country,[294] making this currently the main aspect to be reviewed in the assessment of the third country's legal system. Another challenge is the adoption of supplementary measures, since the CJEU did not specify what supplementary measures should be taken in order to ensure an adequate level of protection. It is for the data controller or processor to decide whether supplementary measures are necessary in the light of the legal system of the third country, and what supplementary measures are capable of offsetting the impingement of the contractual guarantee caused by the legal system of the third country. The data controller or processor thus face huge uncertainty and risk regarding the appropriateness and effectiveness of the supplementary measures.

2.5.2 The implication of the "Schrems II" judgement on the other appropriate safeguards

Though the "Schrems II" judgement is merely directly concerned to the standard data protection clauses, its implication is not limited to the standard data protection clauses. At least regarding the application of the binding corporate rules, it is the EDPB opinion that the CJEU's ruling also applies in the context of the binding corporate rules.[295] Meanwhile, the EDPB did not secure the application of the judgement on other transfer tools under Art. 46 other than SCCs and binding corporate rules. It merely stated that it will assess the consequences of the judgement on the other transfer tools.[296] In another official document of the EDPB, the "Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data" (hereinafter referred to as the "Recommendation on Supplementary Measures"), the EDPB's recommendations direct at all transfer tools under Art. 46.[297] The EDPB also stated in this Recommendation on Supplementary Measures that the transfer tools under Art. 46 only contain contractual guarantees, the legal system in the third country may still require the adoption of supplementary measures to ensure an

[294] CJEU, C-311/18, 16.07.2020, para. 135.
[295] EDPB, Frequently Asked Questions on the Judgement of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner *v* Facebook Ireland Ltd and Maximillian Schrems, 23 July 2020, question 6).
[296] Ibid, question 7).
[297] EDPB, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, Version 2.0, adopted on 18 June 2021.

essentially equivalent level of protection.[298] Against this backdrop, it is rather unclear and confusing, whether and how the CJEU's aforementioned ruling should apply to transfer tools other than SCCs and binding corporate rules under Art. 46, in particular to the codes of conducts and certification mechanisms.

2.5.3 The Recommendation on Supplementary Measures

In order to help the data controller or processor to assess the legal system of the third country and identify necessary supplementary measures, the EDPB has adopted the Recommendation on Supplementary Measures on 18 June 2021. In this Recommendation on Supplementary Measures, a road map of the steps to take in order to identify the necessary supplementary measures is provided. Besides, it also contains an annex 2 that lists some concrete examples of supplementary measures that might help to ensure an essentially equivalent level of protection in the third country.

According to the EDPB's recommendation, the first step is to know the data transfer.[299] The second step would then be to identify the transfer tools, namely whether the transfer is relied on an adequacy decision, the derogations under Art. 49, or the appropriate safeguards under Art. 46.[300] If a transfer is based on the appropriate safeguards under Art. 46, the data controller or processor needs to continue with step 3.[301] In step 3, the controller or processor has to assess whether the used transfer tool under Art. 46 is effective in light of all circumstances of the transfer.[302] To that end, the controller or processor need to pay attention to the characteristics of the transfer itself, as well as the relevant applicable laws of the third country to that transfer.[303] When reviewing the applicable laws of the third country, the controller or processor needs to assess whether the obligations arising from such laws contradict to the commitments contained in the relied transfer tool, thus impinge on the effectiveness of the transfer tool.[304] One should in particular pay attention to the laws granting the public authorities in the third country

[298] Ibid, para. 21-23.
[299] Ibid, para. 8-13.
[300] Ibid, para. 14-27.
[301] Ibid, para. 27.
[302] Ibid, para. 28-44.
[303] Ibid, para. 28-31.
[304] Ibid.

access to the personal data transferred, and assess whether such granting of access is limited to what is necessary and proportionate in a democratic society, with the help of the EDPB's European Essential Guarantees.[305] If the result of the assessment leads to the need of supplementary measures, step 4 is then to adopt appropriate supplementary measures. [306] The EDPB listed some examples of technical, contractual and organisational supplementary measures in annex 2. Step 5 is to go through the procedural steps.[307] It is worth noting that in this part, the EDPB merely mentioned the potential procedural steps in the case of SCCs, binding corporate rules and ad hoc contractual clauses. The other two transfer tools, namely codes of conduct and certification mechanisms, which also come into appearance in step 2, are not mentioned at all. In the author's opinion, this reveals the uncertainty of the EDPB which kind of consequence the CJEU's requirement of taking supplementary measures has on codes of conduct and certification mechanisms. The last step is to re-evaluate the level of protection at appropriate intervals.[308]

It is acknowledged that the Recommendation on Supplementary Measures with its roadmap of the steps to assess and identify supplementary measures is an effort generally welcomed and provides more guidance for data controllers and processors, legal practisers and supervisory authorities against the backdrop of huge legal uncertainty left behind by the "Schrems II". The roadmap it has developed builds the theoretical framework for conducting the assessment of the legal system of the third country and the supplementary measures. However, it has also given rise to concerns and critics by various stakeholders. Among the comments made by industry association and data protection legal counsels, a common concern is that the requirements imposed on the data exporter is unrealistically burdensome, in particular in terms of the assessment of the surveillance laws of the third country, since even the Commission need years to carry out an assessment in the context of an adequacy decision.[309] Also

[305] Ibid, para. 35-42.
[306] Ibid, para. 50-58.
[307] Ibid, para. 59-66.
[308] Ibid, para. 67-68.
[309] DLA PIPER, DLA Piper Comments on EDPB Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data (Public Consultation Reference R01/2020), 21 December 2020, section 4; Joint Comments by SRIW, Scope Europe and the EU Cloud Code of Conduct, Comments on EDPB Public Consultation R01/2020: 'Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data', December 2020, section 3.3; European Federation of Data Protection Officers, Comments on the EDPB Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of

the listed examples of use cases of technical, contractual and organizational are considered by the commentators as unrealistic and not sufficiently specific.[310] Lastly, it is also noted by the commentators that the self-regulatory schemes, such as the codes of conduct and certification mechanisms are not addressed by the EDPB's Recommendation, further ignoring and undermining the function of the codes of conduct and certification mechanisms as a transfer tool.[311] Due to these deficiencies, even after the Recommendation on Supplementary Measures is issued, the fate of data transfers based on appropriate safeguards is still uncertain. In worst case, the data exporter has to suspend the data transfer and keep the data within the EU.

2.5.4 The new SCCs

On 4 June 2021, the Commission officially adopted the New SCCs.[312] The New SCCs contain four sets of SCCs tailored to four data transfer modules respectively: data transfer from controller to controller, data transfer from controller to processor, data transfer from processor to sub-processor, data transfer from processor to controller.[313]

Following the "Schrems II" judgement, the New SCCs have extended and specified the obligations of the data exporter and importer regarding the assessment of the legal system of the third country, by containing a special clause titled "Local laws affecting compliance with the Clauses" and another clause titled "Obligations of the data importer in case of access by public authorities". According to these two clauses, the parties have to warrant that they have no reason to believe that the local laws in the third country would prevent the data importer from fulfilling its obligations under the clauses, taking into consideration the specific circumstances of the transfer, the relevant

Personal Data, 22 December 2020.
[310] Ibid.
[311] DLA Piper, DLA Piper Comments on EDPB Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data (Public Consultation Reference R01/2020), 21 December 2020, section 1 point 1; Joint Comments by SRIW, Scope Europe and the EU Cloud Code of Conduct, Comments on EDPB Public Consultation R01/2020: 'Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data', December 2020, section 3.5.
[312] Commission Implementing Decision (EU) 2021/914 of June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, adopted on 4 June 2021.
[313] Ibid.

laws in the third country and the adoption of necessary supplementary measures.[314] To make such assessment, the data import has to provide the data exporter with relevant information and notify the data exporter of any changes which might lead to a different assessment result.[315] Following such notification of the data importer, the data exporter must promptly adopt appropriate supplementary measures to address the issue, or, if no appropriate supplementary measures can be identified, the data exporter has to suspend the transfer.[316] Besides, the data importer also agrees to notify the data exporter and the data subject, if it has received a request to access the transferred data from the public authorities. The data importer further warrants to review and challenge the legality of such request before cooperate with it, and only provide the minimum information required by the request.[317]

As noted by the CJEU, the standard data protection clauses only provide contractual guarantees between the parties, and their validity depends on whether the clauses contain effective mechanisms that make it possible to ensure compliance with the level of protection required by EU law, and make sure that the data transfers are suspended in the event of breach of the clauses.[318] In the light of this standard of the CJEU, it seems like the SCCs have two main tasks: first, to obligate the data importer in the third country to process the personal data transferred in accordance with the GDPR, and second, if the data importer is not able to fulfill this obligation, the data exporter should be well informed and be able to give up or suspend the data transfer. Under the New SCCs, the first task is addressed by Section II concerning the material data protection safeguards that must be abided by the parties, and the second task is addressed by Section III Clause 14 concerning the local laws affecting compliance with the Clauses and Clause 15 concerning the obligations of the data importer in case of data access by public authorities. In particular the latter reflects the requirements set by the CJEU in "Schrems II". Compared to the three sets of SCCs adopted under the Data Protection Directive ("the Old SCCs"), under the New SCCs, both the obligations of the data exporter and the data importer in the assessment of the legal system of the third country are enhanced. Whereas in the Old SCCs, only the data importer has to warrant that he

[314] New SCCs, Section III Clause 14 (a) and (b).
[315] New SCCs, Section III Clause 14 (c) and (e).
[316] New SCCs, Section III Clause 14 (f).
[317] New SCCs, Section III Clause 15.2 (a).
[318] CJEU, C-311/18, 16.07.2020, para. 137.

has no reason to believe that the laws in the third country would prevent him from fulling his obligations under the clauses,[319] under the New SCCs, both parties have to make the warranty and conduct the assessment regarding the legal system of the third country jointly. The exporter is further obligated to identify appropriate supplementary measures, engage in the data protection supervisory authority, and in worst cases, suspend the data transfer, if the laws in the third country impinge on the obligations laid down in these clauses. These obligations of the parties are in line with the CJEU's ruling in "Schrems II", which states that it is for the controller or processor in collaboration with the recipient of the data to verify whether the law of the third country ensures adequate protection.[320] In addition, the various information and notification obligations of the data importer should help the data exporter to make the assessment and identify any necessary supplementary measures. It is worth noting that, when assessing the impact of the laws and practices of the third country on compliance with the New SCCs, the footnote of Section III Clause 14 (b) provides that "different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame"[321]. This seems to indicate that the Commission takes the position that the practical possibility of certain kinds of personal data being accessed by public authorities should be considered when assessing the data access by public authorities. It is unclear whether an assessment can be made on the ground that the data importer as well as other data importers in the like have never received a request for disclosure from public authorities. Especially, when the laws of the third country regulating data access by public authorities are so vague that they theoretically do not exclude such requests.

In the end, the significance of the update of the SCCs must not be overestimated for the purpose of establishing a practically workable legal framework for data transfer based on appropriate safeguards after the "Schrems II", since even the Old SCCs were considered valid in "Schrems II". The content of the SCCs themselves were never the problem in "Schrems II", the real problems were and remains in the "after 'Schrems II'"

[319] For example, Commission Decision 2001/497/EC, Clause 5 (a).
[320] CJEU, C-311/18, 16.07.2020, para. 134.
[321] New SCCs, Section III Clause 14 (b) footnote.

era, whether the laws of the third country contradict with the obligations and warranties contained in the SCCs, thus causing the SCCs ineffective, and whether such ineffectiveness of the SCCs caused by the laws of the third country can be compensated with supplementary measures. The data controller or processor still needs to deal with these problems, even after the New SCCs are officially adopted.

2.6 Derogations from the adequate protection

In the absence of an adequacy decision and if the adoption of appropriate safeguards is infeasible or impossible, a data transfer to a third country may also take place if one of the derogations laid down in Art. 49 section 1 GDPR applies to it. However, as noted above, since the application of the derogations does not provide any extra guarantees to the data transferred to a third country, the data controller or processor should first endeavor to use the frameworks that provide guarantee of adequate protection or appropriate safeguard to the natural persons after their personal data are transferred to a third country. Is there a feasible possibility to adopt appropriate safeguards and the data controller or processor base the data transfer on a derogation instead of an appropriate safeguard, the data controller or processor might face accusations of non-compliance with the GDPR.

In addition, the application conditions of the derogations must be interpreted restrictively.[322] Among the 8 derogations laid down in Art. 49 section 1, recital 111 correspondent to Art. 49 has required that, the derogations with regard to a contract obligation or legal claim only apply to the transfers that are "occasional and necessary".[323] Recital 113 further states that, transfers that are "not repetitive and only concern a limited number of data subjects" could be carried out based on compelling legitimate interests pursued by the controller, when those interest are not overridden by the interests or rights and freedoms of the data subject.[324] The EDPB has interpreted this "occasional" and "not repetitive" requirement as, the transfers "may happen more

[322] EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25 May 2018, p. 4.
[323] Recital 111, GDPR.
[324] Recital 113, GDPR.

than once, but not regularly, and would occur outside the regular course of actions".[325] In any event, if there is a stable relationship between the data exporter and the importer, the data transfer carried out within this relationship would very likely be deemed as repetitive. For other derogations, namely the "explicit consent of the data subject", "important reasons of public interest", "vital interests of the data subject or of other persons" and "public register", there is no such requirement mentioned under Art. 49. Nevertheless, the EDPB has stressed that these derogations must also be interpreted in a way conforming to the nature of the derogations as exceptions.[326]

IV. Features and Functions of the Data Transfer Rules Compared to the Direct Application of GDPR

From the above, it can be observed that the data transfer rules under Chapter V GDPR are directed at the risks associated with the location of the personal data and the data controller or processor in a third country.[327] These risks lie in particular in the difficulties in the exercise of the data subjects' rights, the enforcement of legal liabilities against the data controller or processor in the third country in the event of non-compliance, and the unauthorized access to the personal data by the public authorities in the third country. These risks and problems are addressed and responded with in the adequacy assessment and conditions for appropriate safeguards. In this sense, against the opinion of not necessary to apply two similar sets of rules of the same purpose to the same data flow, taking into account the enforcement problems identified in chapter 2, this dissertation comes to the conclusion that it makes sense to allow Art. 3 and Chapter V GDPR apply simultaneously to the same data flow, including for the data transfers from the EU data processor to the non-EU data controller and that from the EU data subject to the non-EU data controller. Based on the analysis all above, the reasons are mainly twofold:

[325] Ibid, p. 4.
[326] Ibid, p. 3.
[327] Same opinion on HON, W. Kuan; MILLARD, Christopher, Data Exports in Cloud Computing-How Can Personal Data be Transferred Outside the EEA? The Cloud of Unknowing, Queen Mary School of Law Legal Studies, Research Paper No. 85/2011, p. 34.

1. The enforcement problem arising from the application of Art. 3

Under the direct application of the GDPR, the non-EU data controller or processor has to comply with all the principles and obligations laid down by the GDPR just as any other EU data controllers or processors. In other words, a non-EU data controller or processor is treated the same as an EU data controller or processor. This result seems to make total sense. What problematic is, whether a non-EU data controller or processor really is at the same position as an EU data controller or processor. This must be answered in negative when one recalls the extra problems brought by the non-EU-location of the data controller or processor and the personal data. Whereas the non-EU-location of the data controller or processor is responded with the obligation to designate a representative in the EU, the non-EU-location of the personal data of the EU data subjects after the transborder data flow is not addressed by Art. 3 at all. Even in the former case where an obligation to designate a representative in the EU exists, the enforcement of such obligation is problematic.

As demonstrated in chapter 2 of this dissertation, though the GDPR may directly apply to the processing of personal data by non-EU controllers or processors, the enforcement of it is a genuine problem that has little prospect to be solved under the current stand and in the near future. First, the limited resources of the supervisory authorities inevitably lead to the result that the investigation of violations against the GDPR by non-EU data controllers or processors would only be random. Second, as demonstrated, the supervisory authorities also lack the legal basis to enforce the GDPR in a third country due to international law restrictions. Since there are no extra obligations imposed on the controller established outside of the EU prior to the data transfer to the third country, if violations against the GDPR occur in the third country, the rights of the data subject could hardly be exercised in the practice due to these enforcement difficulties.

The application of the data transfer rules under Chapter V GDPR to the data flow would make up a constructive step towards a solution to the above enforcement problem. This is because, while the sanction against existing violations and remedy for damages under

the direct application of the GDPR is *ex post facto*, the application of data transfer rules provides an extra layer of protection prior to the data transfer to the third country. Besides, the cross-border enforcement of contractual liabilities between two private parties is easier than direct enforcement actions taken by such public authority as the data protection supervisory authorities. This can be further elaborated as the following:

1.1 Adoption and enforcement of appropriate safeguards

Chapter V GDPR requires that personal data could only be transferred to a third country, if the data protection level of that third country is adequate, otherwise appropriate safeguards, mostly by means of contract or certification, must be in place. Since the most countries have not yet received an adequacy decision from the EU Commission, the data transfer to a recipient in these countries could only be carried out with appropriate safeguards or base on a derogation in exceptional cases.

Art. 46 provides as appropriate safeguards for private data controllers or processors mainly four possibilities: standard data protection clauses, binding corporate rules, approved code of conduct and approved certification mechanism. The requirement to adopt these appropriate safeguards can be understood as a threshold to avoid unexamined data transfers to a random recipient in a third country, which forces the data controller in the third country to take extra, concrete efforts and measures before it can actually get the data. This is particularly important, when there is no data controller within the EU as the first contacting and responsible point for any possible future violations and damages. In particular when the last two safeguards are taken, it means that the non-EU data controller is subject to an approved code of conduct or has received approved certification. This factually picks out data controllers in the third country that are conscious about the protection of personal data and already have their data protection compliance checked by independent bodies. In this sense, the requirement of adopting appropriate safeguards provides an extra, prior layer of protection for the data processing in the third country.

In addition, the adoption of appropriate safeguards generally brings two private entities (most probably commercial companies or organizations) together to build a civil

relationship, either through SCCs with another party or through adherence to a code of conduct or certification with the body that is accredited for that purpose. If an unlawful processing or misuse of data is conducted by the data controller or processor in the third country, it will most probably also violate the contract or the code of conduct or the certification conditions. Against this background, if damages occur, the party located in the EU, the association that manages the code of conduct or the certification body could hold the data controller in the third country liable based on the contract or the certification conditions. Further, since the party located in the EU of the contractual mechanisms or the association that manages the code of conduct or the certification body is usually a company or organization, some of them even have offices globally, they have more resources and are more motivated to hold the data controller or processor in the third country liable, especially when they themselves have suffered damages from the unlawful processing by the data controller or processor in the third country.

1.2 Stricter conditions required by the derogations

Even if appropriate safeguards are not available and the data transfer could only take place upon the derogations, the conditions for a data transfer to a third country are mostly more stringent than the conditions required for a simple processing, which must be in place under the direct application of the GDPR. For instance, whereas consent as a legal basis for a simple processing does not have to meet other additional conditions,[328] consent as a legal basis for a data transfer to a third country has to be explicit.[329] Besides, the data subject must also be specifically informed of the intended transfer as well as the risks of such transfer due to the absence of an adequacy decision and appropriate safeguards.[330] Therefore, even if the derogations are the only choice, it still makes sense to apply them instead of the less stringent legal bases for simple processing operations.

[328] Art. 6 section 1 (a), GDPR.
[329] Art. 49 section 1 (a), GDPR.
[330] Ibid.

2. The subjection of the non-EU data controller to the law of the third country

Even if the non-EU controller is subject to the GDPR per Art. 3, since it is established in a third country, it has to comply with the law of that third country. In this case, it is possible that the law of the third country would have different or even contradictive rules from that of the GDPR with regard to the processing of the personal data. For example, where the GDPR encourages or requires anonymization of the personal data in many places and to delete them after a certain period, the Chinese real-name registration system requires some data controllers to collect and keep record numerous identification data of the data subject, in particular in the communication or social media sector.[331] Where such different rules exist, the non-EU data controller would be more motivated to comply with the law of their home country, since the risk of being sanctioned or enforced in the EU is much slighter than in its home country. In such cases, the compliance obligation with the GDPR might be neglected.

As stated in the previous section, this is exactly the CJEU's concern in "Schrems II". This concern is mainly caused by the fact that the personal data is now located in a third country, so that the public authority in that country, including governmental and judicial authorities, have facilitated access to the data, compared to the case where such data is located in the EU. As mentioned above, this concern is not addressed by Art. 3.

In contrast, the access of the public authorities in a third country to personal data is an important criterion for any assessment of adequate level of protection under chapter V of the GDPR. Not only an adequacy decision assessment must pay attention to it, the CJEU has confirmed in "Schrems II" that, in the case of a data controller or processor transferring personal data based on the appropriate safeguards, the controller or processor must also assess the laws in the third country regulating data access by the public authorities, and if necessary, take supplementary measures to ensure an adequate level of protection of the personal data transferred.[332] Even though it is still somewhat

[331] For example, Provisions on the Administration of Internet User Public Account Information Services, Cyberspace Administration of China, effective from 09.10.2017.
[332] CJEU, C-311/18, 16.07.2020, para. 134.

unclear what kinds of supplementary measures can be taken by the data transferring parties to deal with the access of the public authorities in a third country, the issue is at least confronted with under Chapter V and has caught even more attention after "Schrems II", which can be generally seen as an improvement compared to Art. 3.

3. Mid-conclusion

To sum up, it is uncontroversial that Chapter V GDPR applies when a EU data controller or processor transfers personal data to a non-EU data controller or processor. This scenario is not covered by Art. 3, if the non-EU data controller or processor only receives the data from the EU data controller or processor, which itself does not fulfill the conditions laid down in Art. 3. Far less clear is the case where Art. 3 already applies to the data processing involved, so that the data controller outside of the EU is subject to the GDPR with regard to that data processing. In the cross-border E-Commerce context, this is in particular reflected in the circumstances where the data are sent from an EU data processor to a non-EU data controller that is subject to the GDPR, or from the data subject to a non-EU data controller that is subject to the GDPR. In such cases, whether the data transfer rules under chapter V GDPR should still apply is disputed in the literature. After examining the application conditions of Art. 3, this dissertation has underlined the enforcement problem resulted from the application of Art. 3. It further argues that due to this enforcement problem and other problems resulted from the location of the personal data in the third country, Art. 3 alone is not able to provide a sufficient level of protection of personal data in a third country. It makes sense to combine Art. 3 and the data transfer rules laid down in Chapter V in order to achieve a better protection of personal data of the EU data subjects in the third country.

It follows that, if Chapter V GDPR is to apply to the above-mentioned data flows from an EU data processor to a non-EU data controller that is subject to the GDPR, or from the data subject to a non-EU data controller that is subject to the GDPR, what kinds of legal bases can be relied upon to carry out the data transfer.

Bearing this question in mind, the following chapter will first assess, due to the focus of this dissertation of the data flows from the EU to China, the data protection level in

China. It will then discuss whether an adequate level of data protection to the EU can be awarded to China, whether for the whole country or just for a specific branch such as the E-Commerce branch.

Chapter 4 Data Protection Level in China in Comparison to the EU

I. Global Data Protection and Data Protection Development in China

Few law fields have attracted so much attention and undergone so strong transformation in the last decades as data protection. Starting from Sweden's first comprehensive national data privacy law in 1973, after a development of about 50 years, today 107 countries (64% of all countries) already have data privacy legislation in their legal system[333]. In this sense, intensified legislation on data protection and privacy has become a worldwide trend, instead of a phenomenon merely exists in certain modernized regions. Data protection belongs to the young but fastest developed fields in the global legal landscape.

1. Global data protection trend

Except for the EU Member States, whose national data protection laws are to a great extent harmonized by the GDPR, the exact contents of the data protection legislations vary from country to country and from region to region, just like any other legal field which is not yet globally harmonized, for each country has its own social and legal

[333] Data from the United Nations Conference on Trade and Development, available under https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx, last visited on 10.11.2020.

characters, which may be comparable but not identical. However, focusing on the general picture instead of the details, some commentators have observed that there are some common elements in the data protection legislations in different countries.[334] This is at least partly because most national data protection legislations were more or less shaped by the principal international instruments concerning personal data protection, notably the 1981 Council of Europe Convention on Data Protection, the OECD Privacy Guidelines and the APEC Privacy Framework, and these international instruments share some common principles or codes.[335]

However, despite the existence of some common principles in most national data privacy laws, the level of data protection in each jurisdiction is not always equivalent. On one side, some nations or regions may have adopted more data processing principles than the others, on the other side, even if the same data processing principles are adopted, they may be construed varyingly stringently in different legal systems. Besides, there are also other factors that could affect the actual level of the protection to personal data in a jurisdiction, such as the enforceability of the adopted data protection rules.

Among the various data protection laws in different countries or regions, it is well recognized that the EU Data Protection Directive adopted in 1995 established a high-level legal framework for the protection of personal data, the in 2018 effective GDPR remained and further enhanced such high-level protection. Through this two legislation instruments and the predated 1981 Council of Europe Convention on Data Protection, the EU has developed its own data protection standards that are called by the data protection specialist Prof. Graham Greenleaf as the "European Standards".[336] The European Standards are derived from the comparison of the EU data protection law and the aforementioned OECD Privacy Guidelines and APEC Privacy Framework, referring to those elements that do not exist in those international agreements but exist in the EU data protection law.[337] These European Standards are the general manifestations of EU's high level of protection to personal data. EU's high level of data

[334] Lee A Bygrave, Privacy and Data Protection in an International Perspective, Scandinavian studies in law, Vol. 56, 2010, p.199.
[335] See Lee Andrew Bygrave, "Data Privacy Law: An International Perspective", Oxford University Press, Oxford, 2014. P. 1.;
[336] GREENLEAF, Graham, The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108; International Data Privacy Law Vol. 2, 2012, p. 73.
[337] Ibid.

protection reflects itself not only in the substantive rules written in the data protection law, but also in its status as a fundamental right, and the strict enforcement mechanisms implementing the data protection law in the real world.

2. Data protection development in China

Unlike in the EU, China has a much shorter legal tradition in data protection law. China's first attempt to adopt a comprehensive data protection law was in 2003, which only resulted in two scholarly drafts and were never adopted as legislation.[338] After that, only scattered, sectoral laws and regulations were adopted that contain provisions on the protection of personal data. The scattered rules related to the protection of personal data mainly find itself in the new Chinese "Civil Code" which came into force on 1 January 2021, the Cyber Security Law, the Criminal Law, the Consumer Law as well as in other sector specific fields, for instance in the E-Commerce field. Recently, on 20 August 2021, both driven by the worldwide data protection legislation trend and the urgent need within China for enhanced data protection, China has passed its first comprehensive "Personal Information Protection Law" ("PIPL"), which came into effect on 1 November 2021. The following part will scrutinize the material Chinese data protection rules as per its current stand. Comparisons to the GDPR will be made when differences are detected.

However, first of all, it needs to be noted that the term "personal data" is not commonly used in the Chinese law, instead, "personal information" is the official concept adopted in Chinese data protection law. Personal Information is defined in the "Cybersecurity Law of the P.R.C" and PIPL as the information referring to "various types of information that can be used separately or in combination with other information to identify a natural person, including but not limited to the name, date of birth, identity certificate number, personal biological identification information, address, telephone

[338] The two drafts were published as: QI, Aimin (齐爱民), Model Law on the Personal Information Protection Law (Scholar Draft) (中华人民共和国个人信息保护法示范法草案学者建议稿), Hebei Law Science (河北法学), 2005, No. 6, p. 2-5; ZHOU, Hanhua (周汉华), Personal Information Protection Law (Scholar Draft) (个人信息保护法（专家建议稿）及立法研究报告), Law Press (法律出版社), 2006.

numbers, etc. of the natural person".[339] Apparently, this concept in the Chinese law is essentially similar to the European definition "personal data". In the following, for consistency reasons, this dissertation will continue to use "personal data" instead of "personal information" under the Chinese law context.

2.1 Data protection as a fundamental right in China?

2.1.1 The right to the protection of personal data as a fundamental right in the EU

The high-level protection of personal data in the EU is largely due to and manifested in its fundamental right status. The right to the protection of personal data was not a fundamental right in the EU at the beginning. In the Data Protection Directive, the protection of personal data was directly linked to the right of privacy, a fundamental right enshrined in the European Convention of Human Rights (Article 8). the Data Protection Directive never expressed the protection of personal data itself as a fundamental right.

It remained so until the Lisbon Treaty in 2009 brought into force the EU Charter of Fundamental Rights, which enjoys the same legal value as the constitutional treaties of the EU[340]. The EU Charter of Fundamental Rights treats the right of privacy and the right to the protection of personal data as two separate fundamental rights for the first time.[341] Furthermore, Art. 16 of the Treaty on the Functioning of the European Union obliges the EU legislators to lay down data protection rules for the processing of personal data.[342] Against this background, Recital 1 of the GDPR expressly state that "the protection of natural persons in relation to the processing of personal data is a fundamental right".

[339] Art. 76 (5), Cybersecurity Law of the P.R.C.
[340] See: European Data Protection Supervisor, Data Protection, available at https://edps.europa.eu/data-protection/data-protection_en, last visited on 09.09.2023.
[341] Art. 7 and Art. 8, EU Charter of Fundamental Rights.
[342] See https://edps.europa.eu/data-protection/data-protection_en, last visited on 18.01.2021.

2.1.2 Function of the fundamental right

The Charter of Fundamental Rights of the European Union are binding to all EU institutions and bodies of the EU, as well as to the Member States when implementing Union law.[343] These bodies of the EU and the Member States have to "respect the fundamental rights, observe the principles and promote the application thereof in accordance with their respective powers". [344]

The right to the protection of personal data evolving into a fundamental right of the EU has a significant impact on the relationship between the state, the data subject and the other third parties. Generally speaking, fundamental rights of the EU are derived from the human rights commonly recognized in the EU and the constitutional traditions rooted in the EU Member States.[345] In this sense, according to the human rights law theory, the EU has both positive and negative obligations to ensure its citizens fundamental rights. [346] The negative obligations require the EU to respect the fundamental rights and refrain from conducts that might infringe them.[347] On the other side, the positive obligations obligate the EU to protect and promote the fundamental rights of its citizen, this include in particular to prevent the fundamental rights from being violated by a third party, including the third parties outside of the EU territory.[348] Given these effects of the fundamental rights, the right to the protection of personal data being recognized as a fundamental right primarily protects the citizens from the excessive or illegal data processing activities of the State. Thus, the EU data protection law applies to the data processing activities carried out by the public authorities. Second, as a result of the positive obligation, EU data protection law must also prevent the right to the protection of personal data being violated by private data controllers or processors. Thus, the EU data protection law also applies to the data processing activities of private data controllers or processors.

---

[343] Art. 51, Charter on the Fundamental Rights of the European Union.
[344] Ibid.
[345] TAYLOR, Mistale, The EU's Human Rights Obligations in Relation to its Data Protection Laws with Extraterritorial Effect, International Data Privacy Law, 2015, Vol. 5, p. 246-256.
[346] Ibid, and also MILANOVIC, Marko, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, Harvard International Law Journal, 2015, Vol. 56, p. 81.
[347] Ibid.
[348] Ibid.

2.1.3 Limitation on fundamental rights

The right to the protection of personal data being a fundamental right in the EU makes sure that personal data of the EU data subjects enjoy a high level of protection. This is guaranteed by the stringent conditions that are imposed on the limitation to fundamental rights. According to Art. 52 of the EU Charter of Fundamental Rights, the restriction of fundamental rights must be provided by law and respect the essence of the fundamental rights.[349] Besides, the restriction must be proportionate, i.e., relevant and necessary for the objectives it pursues. Thus, Art. 52 raises two general restrictions on the restriction of fundamental rights, namely the restriction of fundamental rights must respect the essence of the restricted fundamental rights and be proportionate.

In terms of the relationship between the essence requirement and proportionality, there is a relative and an absolute theory in the German doctrine.[350] According to the absolute theory, the essence of a fundamental right cannot be limited. If the essence of a fundamental right is compromised, the fundamental right is infringed, no further examination of proportionality will be needed.[351] The case law of the CJEU seems to have followed this absolute theory in the *Schrems I* case.[352] A fundamental right can never be totally excluded even if it has to be balanced against other fundamental rights. Even according to the relative theory, the interference of a fundamental right still needs to go through the proportionality test. The stronger the essence of a fundamental right is compromised, the heavier the counter-interest must be.

With regard to the right to the protection of personal data, the above theories mean that there are stringent limits on the restriction of the right to the protection of personal data. In any case, the right to the protection of personal data should not be entirely overlooked, even if the other interest in the stake is something as big as public interest or national security. Restrictions could be imposed in certain circumstances depending on the counter-interest, however, if the restriction on the right to the protection of personal data is so strong that it empties the protection of personal data, such restriction will

[349] Art. 52 section 1 of the Charter of Fundamental Rights.
[350] BRKAN, Maja, The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core, European Constitutional Law Review, 2018, Vol. 14, p. 336.
[351] LENAERTS, Koen, Limits on Limitations: The Essence of Fundamental Rights in the EU, German Law Journal, 2019, Vol. 20, p. 781.
[352] Ibid.

violate the fundamental right to the protection of personal data of the EU data subjects. An example hereof is the finding of the CJEU in the *Schrems I* case[353], where the CJEU states that "legislations permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life"[354]. The CJEU decided that the USA does not provide an adequate level of protection to the personal data partly on this reason.

2.2 Influence of the fundamental right approach in China

In China, the protection of personal data is not expressly provided for in the Chinese Constitution, in any case not in the Chapter 2 of the Constitution "the fundamental rights and obligations of the citizens". However, some scholars hold the opinion that a right that is not explicitly provided for in the Constitution could still have fundamental nature, if it can be deducted from the general provisions concerning the rights of the citizens, since the Constitution is usually made a long time ago and could not include all new rights that gained weight with the development of the society.[355]

In recent years, the German doctrine of the informational self-determination has gained popularity in Chinese legal theory.[356] In Germany, the fundamental right to informational self-determination was first established by the German Federal Constitutional Court in the "Volkszählung (in English: census)" case in 1983. In this case, the Court decided that, under the conditions of modern data processing, the

---

353 CJEU, C-362/14, 06.10.2015.
354 CJEU, C-362/14, 06.10.2015, para. 94.
355 YAO, Yuerong (姚岳绒), On the Justification of the Right of Information Self-determination as a Basic Right in China (论信息自决权作为一项基本权利在我国的证成), Political Science and Law (政治与法律), 2012, No. 4, p. 73; SUN, Ping (孙平), Systematic Construction of the Fundamental Right Model of Personal Information Protection Legislation (系统构筑个人信息保护立法的基本权利模式), Law Science (法学), 2016, Vol. 4, p. 67; TU, Zhenyu (屠振宇), Research on the Right to Privacy in the Constitution (宪法隐私权研究), Law Press (法律出版社), 2008, p. 176-187; WANG, Xiuzhe (王秀哲), Research on the Constitutional Protection of the Right of Privacy (我国隐私权的宪法保护研究), Law Press (法律出版社), 2011, p. 38-46.
356 See YAO, Yuerong (姚岳绒), On the Justification of the Right of Information Self-determination as a Basic Right in China (论信息自决权作为一项基本权利在我国的证成), Political Science and Law (政治与法律), 2012, No. 4, p. 72-83; ZHAO, Hong (赵宏), The Status Quo of the Protection of Information Self-Determination in my Country and the Prospect of Its Legislation (信息自决权在我国的保护现状及其立法趋势前瞻), China Law Review (中国法律评论), 2017, No. 1, p. 147-161.

protection of the individual against unlimited collection, storage, use and disclosure of his or her personal data is covered by the general right of personality under Article 2 I in conjunction with Article 1 I Basic Law for the Federal Republic of Germany. In this respect, the individual has a fundamental right to determine for himself or herself the disclosure and use of his or her personal data. Restrictions on this right to informational self-determination are only permissible if there is an overriding public interest. In addition, any legislative restriction on the fundamental right requires a constitutional legal basis, which must comply with the constitutional requirement of clarity of norms. The legislator must also observe the principle of proportionality. It must also take organizational and procedural precautions which counteract the danger of a violation of the right of personality.[357] Since the fundamental right to informational self-determination is not explicitly laid down in the Basic Law for the Federal Republic of Germany, but is derived indirectly from Article 2 I in conjunction with Article 1 I of the Basic Law for the Federal Republic of Germany, Chinese scholars argue that the same fundamental right to the protection of personal data could also be deducted from the Chinese Constitution, namely, from Art. 38[358] (concerning personal dignity) and Art. 33[359] (concerning human rights).[360] The reason and background of this suggestion is the unrestricted massive data processing by the public authorities in China. Apparently, if a fundamental right to the protection of personal data is successfully established, this fundamental right would first of all bind the state power.

As recommendable as this argumentation sounds, the advocators are only several constitution law scholars. Compared to the establishment of the "informational self-determination" as a fundamental right in Germany by the Federal Constitutional Court in the "Volkszählung" case,[361] the protection of personal data has never been discussed

---

[357] Federal Constitutional Court of Germany (BVerfG), Case 1 BvR 269/83, 15.12.1983, para. 74-76.

[358] Art. 38: "The personal dignity of citizens of the People's Republic of China is inviolable. Insult, libel, false accusation or false incrimination directed against citizens by any means is prohibited."

[359] Art. 33 sentence 3: "The State respects and preserves human rights."

[360] YAO, Yuerong (姚岳绒), On the Justification of the Right of Information Self-determination as a Basic Right in China (论信息自决权作为一项基本权利在我国的证成), Political Science and Law (政治与法律), 2012, No. 4, p. 78; ZHAO, Hong (赵宏), The Status Quo of the Protection of Information Self-Determination in my Country and the Prospect of Its Legislation (信息自决权在我国的保护现状及其立法趋势前瞻), China Law Review (中国法律评论), 2017, No. 1, p.154; SUN, Ping (孙平), Systematic Construction of the Fundamental Right Model of Personal Information Protection Legislation (系统构筑个人信息保护立法的基本权利模式), Law Science (法学), 2016, Vol. 4, p. 67-68.

[361] Fore more details about the case see also Bernard Schlink, The Right of Informational Self-determination (Das Recht der informationellen Selbstbestimmung), Der Staat, 1986, Vol. 25, p. 233.

as a fundamental right in any cases by the Supreme People's Court in China. The Chinese Supreme People's Court is not competent to interpret the Constitution anyway. According to Art. 67 of the Chinese Constitution, the competence to interpret the Constitution lies with the Standing Committee of the National People's Congress, a part of the legislation body. The Standing Committee of the National People's Congress, however, has never made such interpretation with regard to the protection of personal data. In this sense, the proposal to make the protection of personal data a fundamental right is no more than a scholarly opinion, which leaves it still far away from a recognized fundamental right in the Constitution.

In this matter, the new PIPL has brought some new light. Art. 1 PIPL states that the PIPL is issued "based on the Constitution",[362] which seems to speak for the fundamental right approach. Further, it is indicated by the legislator that the protection of personal data is ultimately to protect the human dignity and human right, which is protected by the Chinese Constitution. Thus, it can be argued that the right to data protection is protected by the Constitution in China. In any case, as a result of this development, the application scope of the PIPL has been expanded - it also applies to the data processing activities carried out by public authorities. However, in terms of the constitutional enforcement, it must be noted that even if a right is recognized as a constitutional right, a constitutional review of legislations by an independent court does not currently exist in China. Further, there is no established mechanism for individuals to lodge a constitutional complaint to assert their fundamental rights vis-à-vis the state. Thus, from an EU fundamental right point of view, the constitutional enforcement in China might still be deficient.

II. Substantial Data Protection Rules in China

1. Data protection in the Civil Code

The introduction of the data protection provisions in the Civil Code of the P.R.C. is a young development in Chinese data protection law, since the Civil Code was

[362] Art. 1 PIPL.

promulgated on 28 May 2020 and only became effective from 1 January 2021.

The protection of personal data is governed in Art. 1034-1039 under Chapter 4 "Personality Rights" of the Civil Code. It establishes that the processing of personal data must comply with the principles of lawfulness, fairness and necessity.[363] The processing must be consented by the related natural persons unless otherwise stated by laws or administrative regulations; the controller has to disclose the processing rules and the purpose, means and scope of the processing; the processing should be in line with the relevant laws, administrative regulations or the agreement between the parties.[364] In addition, natural persons have a right to access or copy the personal data, when wrong data is detected, the related natural persons can further raise an objection and request for rectification.[365]

These short provisions seem extremely abstract and simple when compared to the comprehensive GDPR. Actually, even these very abstract provisions did not exist in the first draft of the General Part of the Civil Code. The idea of having a data protection provision in the Civil Code first appeared at the Civil Law Colloquia on 10. October 2016, as some renowned scholars (representing the academy) and People's Congress members (representing the people) proposed to strengthen the protection of personal data through the Civil Code.[366] The introduction of personal data protection in the Civil Code is thus not a primary goal of the legislation body, but rather a response to the dissatisfaction of the people with the ubiquitous personal data misuse which can be observed in the practice.

1.1 Protection of the personal data – a right or legally protected interest?

Although the data protection provisions are put under the chapter "Personality Rights", it is still ambiguous among the civil law scholars whether the protection of personal

[363] Art. 1035, Civil Code.
[364] Ibid.
[365] Art. 1037, Civil Code.
[366] ZHANG, Xinbao (张新宝), Research on Personal Information Protection Provisions in "General Provisions of Civil Law" (《民法总则》个人信息保护条文研究), Peking University Law Journal (中外法学), 2019, Vol. 31, No. 1, p. 54-75.

data is a right of the natural persons, or it is a legally protected interest.

Some scholars argue that the protection of personal data is no more than a legally protected interest.[367] A natural person has no established specific "right" on his or her personal data. According to the systematic structure of the Civil Code, Art. 990 sentence 1 lists an array of specific personality rights, using specifically the wording "right", which does not include a right to the protection of personal data. Art. 990 sentence 2 then goes on stating that except for the personality rights listed above, natural persons also have other personality related interests based on their personal freedom and human dignity that should be protected by the law. If the protection of personal data is not a specific personality right listed in Art. 990 sentence 1, it must be a personality related interest protected by the civil law as per sentence 2. This systematic arrangement is not the result of an accidental overlook, but rather an intentional design.[368] It reflects the legislator's intention to not grant the natural person a strong right to the protection of personal data, but only a comparably weak protection as a legally recognized interest.[369]

However, other commenters consider the protection of personal data as a new right, specifically a new special personality right.[370] They believe that personal data is an important part of the personality of the related natural person, the content of the right to the protection of personal data is determinable and limitable, which includes the right of information, the right of access, the right of rectification *etc.*[371] Also, recognizing the protection of personal data as a personality right contributes to strengthen the protection of personal data, which seems in particular important given the circumstances of the massive data misuse in China today.

---

[367] See LIANG, Huixing (梁慧星), Understanding and Application of the Important Provisions in "General Provisions of Civil Law" (《民法总则》重要条文的理解与适用), Journal of Sichuan University (四川大学学报), 2017, No. 4, p. 51-65; LONG, Weiqiu (龙卫球); LIU, Baoyu (刘保玉), Guidance for Interpretation and Application of the General Provisions of the Civil Law of the People's Republic of China (中华人民共和国民法总则释义与适用指导), China Legal Publishing House (中国法制出版社), 2017, p. 404.

[368] Ibid.

[369] CHENG, Xiao (程啸), Personal Information Protection from the Perspective of the codification of the Civil Code (民法典编纂视野下的个人信息保护), China Legal Science (中国法学), 2019, Vol. 4, p. 26-43.

[370] SONG, Yahui (宋亚辉), Research on Private Law Protection Mode of Personal Information—An Interpretation Theory of Article 111 of the "General Provisions of Civil Law" (个人信息的私法保护模式研究-《民法总则》第111条的解释论), Journal of Comparative Law (比较法研究), 2019, No. 2, p.86-103.

[371] YE, Mingyi (叶名怡), On the Basic Category of Personal Information Right（论个人信息权的基本范畴）, Tsinghua University Law Journal (清华法学), 2018, Vol. 5, p. 143-158.

This dispute, whether the protection of personal data is a specific personality right or a personality related interest protected by the Civil Code, is originally caused by the fact that the protection of personal data is put under the "personality rights", but not expressly referred to as a right. This arrangement seems to indicate that the protection of personal data is a legally recognized personality interest. Under the Chinese civil law dogmatic, the difference between a right and a legally protected interest lays in the insufficient certainty of a legally protected interest.[372] The protection scope of a legally protected interest is blurred and could not provide clear boundary for others, thus should not be raised up to a right.[373] If, due to the development of the dogmatic and the judicial practice, such a legally protected interest can be well categorized to provide pre-definable protection to the concerned natural person and clear guidance for the behavior of others, this legally protected interest may be made into a right.[374] An example of such an interest being upgraded to a right is the right of privacy under the Chinese civil law. In the current stage, the protection of personal data should be considered as a legally protected interest, partially due to the systematic interpretation of Art. 990 as demonstrated above, but also partially due to the huge uncertainties both in the legislation and judicial practice with regard to the protection of personal data. In any case, what is certain is that the protection of personal data is ultimately a protection of the personality of the natural persons.[375]

1.2 Impact of the introduction of the protection of personal data in the Civil Code

Since the protection of personal data is not officially established as a fundamental right under the Chinese Constitution, it is even more important that the Civil Code introduces and places it under the chapter "Personality Rights", which stresses the personality element of the personal data and shows the willingness of the legislators to respect the control of natural persons over their personal data as a personality interest. This

[372] XIONG, Xulong (熊谓龙), Right, or legal interest? -Re-discussion on the Nature of General Personality Rights (权利，抑或法益？－一般人格权本质的再讨论), Journal of Comparative Law (比较法研究)，2005, No. 2, p. 51-57，p. 55.
[373] Ibid.
[374] Ibid, p. 56.
[375] CHENG, Xiao (程啸)，On the Nature of Personal Information Rights and Interests in the Civil Code (论我国民法典中个人信息权益的性质)，Political Science and Law (政治与法律)，2020, Vol. 8, p. 2-14.

personality interest approach is comparable to the German approach, which considers the protection of personal data as a type of the allgemeines Persönlichkeitsrecht (general personality right) within the civil law framework.

From a judicial remedy point of view, the introduction of the protection of personal data in the Civil Code provides a legal basis for the data subject to bring up a civil law proceeding against the infringer. The drawback is that the Civil Code does not specify what kinds of constitutive elements are required for the justification of a tort liability arising from the violation of protection of personal data, which leads to difficulties in determining the infringement and liability.

2. Data protection under the Cybersecurity Law

Another high-hierarchy law governing the collection and use of personal data in China is the Cybersecurity Law of the P.R.C. (hereinafter referred to as the "Cybersecurity Law"), which came into force on 01. June 2017. The three goals of the Cybersecurity Law are to "maintain the cybersecurity and safeguard the cyberspace sovereignty, national security and public interests; to protect the lawful rights and interests of citizens, legal persons and other organizations, and to promote the sound development of economic and social information technology" [376]. This indicates that the Cybersecurity Law first of all serves security, be it national security against international threats, or be it network security in the sense of defending illegal disclosure or network attacks such as hacking. But it also contains some data protection elements. It is important in the sense that it is the first law promulgated by the legislation body that specifies data protection issues, before the PIPL.

The Cybersecurity Law is an internet law. The majority of its provisions refer to the network security and the law only applies to cyberspace, which means, only the collection and use of personal data by a network operator through the network will have to comply with the Cybersecurity Law. Even so, it still deserves a close observation due to several reasons.

[376] Art. 1, Cybersecurity Law.

Firstly, the Cybersecurity Law as a national law has a high position in the hierarchy of the Chinese law system. In addition, the Cybersecurity Law clarifies some basic definitions such as the definition of personal data as well as the rights of the data subject and obligations of the data controller. The Cybersecurity Law itself is highly generalized in terms of the personal data related provisions, but the various implementation regulations and standards do provide more useful guidance. The drawback is that these standards are mostly recommendatory, thus have no binding legal effect. It also lays down rules for the data transfers from China to a third country, which have caused quite a few concerns especially in the foreign invested companies. Therefore, it is necessary to go through the relevant provisions in order to capture a general picture of the data protection law in China.

Before a detailed introduction to the personal data related rules in the Cybersecurity Law and the implementing regulations and standards is made, to avoid misunderstanding, some area-specific notions and terms must be clarified first. Unless otherwise stated, the data protection obligations in the Cybersecurity Law and the implementing regulations and standards only apply to network operators out of all data controllers.[377] Network operators are, according to the Cybersecurity Law, owners and managers of networks and the network service providers.[378] Furthermore, network means "the system that consists of computers or other information terminals and related equipment for collecting, storing, transmitting, exchanging, and processing information according to certain rules and procedures". Since this definition of network is so broad and the Cybersecurity Law does not further elaborate on this matter by giving any example, the scope of network operators is understood very broad in the practice. It includes those who own and manage the infrastructure layer of the internet, like the traditional telecom operators such as China mobile, China telecom and so on. Also network service providers like social media Apps, online platforms, web shops belong to network operators without debate. However, whether companies having their own internal information exchange systems like office email systems or official websites should be considered as network operators, are not always clear. In addition, it is highly ambiguous whether the provisions related to data protection also apply to public

[377] Art. 2, Cybersecurity Law.
[378] Art. 76 (3), Cybersecurity Law.

authorities.[379] The concept of network operator itself does not distinguish between public or private entities. However, as the author has argued elsewhere,[380] the attempt to apply the data protection rules in the Cybersecurity Law to the data collection and use by public authorities in an administrative act would be problematic, since the Cybersecurity Law generally obliges the network operators to obtain consent from the data subject,[381] it is obviously not directed at public authorities performing their public functions, since requiring consent in such cases contradicts to the administrative nature of the public functions. Thus, it is hard to justify that the data protection related provisions in the Cybersecurity Law applies to the public authorities when performing their public functions.

2.1 Principles for data collection and use

Art. 41 of the Cybersecurity Law lays down the principle of lawfulness, fairness and necessity for data collection and use. It requires the network data controllers to publicize the rules for data collection and use, and to clearly indicate the purposes, methods and scope of the data collection and use.[382] Since these principles are the most generally recognized ones for the personal data processing, it shows that the data protection rules in the Cybersecurity Law share some basic characters with the world data protection trend. What notable and probably unique is, Art. 41 generally requires a consent of the data subject for the collection of personal data in all cases.[383] Unsurprisingly, this stipulation is fiercely criticized by scholars. By making reference

[379] Opinions hold that the data protection provisions do not apply to public authorities: SHANG, Xixue (商希雪), Personal Data Sharing beyond Civil rights- An Analysis Based on the Legitimate Interests in the GDPR (超越私权属性的个人信息共享-基于《欧盟一般数据条例》正当利益条款的分析), Studies in Law and Business (法商研究), 2020, No. 2, p. 69; CHEN, Yu-Jie; LIN, Ching-Fu; LIU, Han-Wei, Rule of Trust: The Power and Perils of China's Social Credit Megaproject, Columbia Journal of Asia Law, 2018, No. 1, p. 27; LEE, Jyh-An, Hacking into China's Cybersecurity Law, Wake Forest Law Review, 2018, No. 1, p. 88.

[380] YU, Lu; AHL, Bjorn, China's Evolving Data Protection Law and the Financial Credit Information Systen: Court Practice and Suggestions for Legislative Reform. Hong Kong Law Journal, 2021, Vol. 51, p. 6, available at https://ssrn.com/abstract=3782392.

[381] Art. 41 of the Cybersecurity Law: "When collecting or using the personal information, cyberspace operators shall comply with the principles of legality, justification and necessity, publicize the rules for collection and use, clearly indicate the purposes, methods and scope of the information collection and use, and obtain the consent of those from whom the information is collected. A cyberspace operator shall not collect the personal information irrelevant to the services it provides or collect or use the personal information in violation of the provisions of laws and administrative regulations and the agreements between both parties and shall process the personal information it has stored in accordance with the provisions of laws and administrative regulations and the agreements with the user."

[382] Ibid.

[383] Ibid.

to the data protection laws in other countries, scholars correctly pointed out that requiring consent as a precondition for the collection of personal data in every case is not a common practice in the data protection area.[384] According to these scholars, the over-reliance of consent in the Cybersecurity Law is a result of misunderstanding of the international data protection theory and rules.[385]

Compared to the GDPR, Art. 41 does not contain other basic principles such as purpose limitation, data minimization and storage limitation. However, the aforementioned principles are included in a national commendatory standard titled "Information security technology - personal information security specification" (hereinafter referred to as the "Specification"),[386] which is designed to facilitate the implementation of the Cybersecurity Law. Worth noting is also that, the application scope of this Specification is much broader than that of the Cybersecurity Law, since it applies to all "personal information controller" instead of only "network data controller". This Specification deals with the processing of personal data comprehensively, in this sense, it was considered as the "Chinese GDPR" before the PIPL.[387] What impedes its impact is, of course, its non-bindingness. Data controllers can use it as a guidance, however, the non-compliance with the Specification itself will not lead to sanctions.

In terms of the principles for data processing, the Specification embraces almost the same principles as ensured in the GDPR, including purpose specification, information and consent, necessity and data minimization, transparency, security, accountability and participation of the data subject.[388] Indeed, in an introductory comment of the Specification, one of the drafters explained that during the drafting of the Specification, they have referred to the most recent laws and standards of other countries and international common practices, especially the OECD Privacy Framework, the APEC Privacy Framework, the GDPR, the EU-US Privacy Shield Framework as well as the

---

[384] GAO, Fuping (高富平), Personal Information Protection: From Personal Control to Social Control (个人信息保护：从个人控制到社会控制), Chinese Journal of Law (法学研究), 2018, Vol. 40, p. 84-101.
[385] Ibid.
[386] National Information Security Standardization Technical Committee, Information Security Technology – Personal Information Security Specification (信息安全技术-个人信息安全规范) (version 2020), 06.03.2020.
[387] WANG, Chunhui (王春晖), Comparison of GDPR Personal Data Rights and Personal Information Rights in the Cybersecurity Law (GDPR 个人数据权与《网络安全法》个人信息权之比较), Cyberspace Strategy Forum (网络空间战略论坛)，2018, Vol. 7, p. 43.
[388] Art. 4, Specification.

US Consumer Privacy Bill of Rights.[389]

Despite the general similarities to the GDPR principles, it must be noted that "the devil lies in the details" applies here too. An example hereof is the requirement to valid consent. Whereas under the GDPR a valid consent must be freely given, specific, informed and unambiguous, by a statement or an affirmative action,[390] consent under the Specification can be authorized both by an affirmative action and a negative non-action, for example through the further use of the service or through an "opt-out".[391] Only when sensitive personal data are processed, an explicit consent will be need, namely by a statement or an affirmative action,[392] as required by the GDPR for a normal consent.

2.2 Rights of the data subject

The rights of the individual data subject are set forth in Art. 43. The provision provides the data subject with a right to delete when the network data controller collects or uses his/her personal information in violation of the laws or administrative regulations or the agreements between the parties; a right to rectification if the personal information collected or stored by the network data controller is incorrect.[393]

Then again, the Specification extended the scope of the Cybersecurity Law by granting the data subject more rights, including the right to access, the right to withdraw the consent, the right to delete account as well as the right to obtain a copy of the personal data.[394] Compared to the GDPR, there is no expressly stated right to restriction of processing, right to object and right to data portability contained in the Specification.

[389] YI, Meijin, Comment to the Information Security Technology - Personal Information Security Specification, available under https://www.tc260.org.cn/front/postDetail.html?id=20180201200746, last visited on 10.09.2023.
[390] Art. 4 (11), GDPR.
[391] Art. 3.7, Specification.
[392] Art. 3.6, Specification.
[393] Art. 43, Cybersecurity Law.
[394] Art. 7, Standard.

2.3 Obligations of the network data controller

Besides the obligations corresponding to the rights of the data subject mentioned above, the Cybersecurity Law also imposes an arrange of security obligations on the data controller. Such obligations include a negative prohibition such as not to divulge, tamper with or damage the personal data collected, as well as a positive obligation to adopt technical measures to secure personal data.[395]

In addition, the Specification further imposed organizational obligations to the data controller, including to designate a data protection officer, to keep record of the data processing, to conduct data security impact assessments, to provide data protection related trainings to internal staff as well as to have their data protection policies and practices audited by an independent auditor.[396]

2.4 Data protection supervisory authority

There is no independent data protection supervisory authority under the Cybersecurity Law framework. The Cybersecurity Law only states that the National Cyberspace Administration shall be responsible for the overall planning and coordination of cybersecurity and relevant supervision and administration. Meanwhile, the competent telecommunications department of the State Council, the public security departments and other relevant authorities shall be responsible for cybersecurity protection, supervision and administration within the scope of their respective functions.[397]

According to the above, the National Cyberspace Administration is only a coordinator in terms of cybersecurity issues, the relevant departments themselves are responsible for the supervision and administration within their own functions. This division of competences are highly abstract and uncertain, which causes confusions in individual cases as to which one is the supervisory authority, or all of them if the concerned matter falls within the functions of several departments. Besides, the above division of competences seems only to refer to the cybersecurity, not to the protection of personal

[395] Art 42, Cybersecurity Law.
[396] Art. 11, Specification.
[397] Art. 8, Cybersecurity Law.

data, it is thus unclear whether a natural person could lodge a complaint with regard to the non-compliance of data controller or processor to the relevant departments, if so, to which one. The competences and tasks of the relevant departments are thus far away from clear. Moreover, the above-mentioned departments could hardly be considered independent, since they all have other functions, such as granting license, supervision of other business operations etc. In this sense, it is difficult to justify that the supervision of the data protection compliance by the relevant departments are independent from their other functions in terms of personal and resources.

2.5 Administrative and judicial remedy

Under the GDPR, the data subject has a right to lodge a complaint with a supervisory authority.[398] Without prejudice to this administrative remedy, the data subject also has a right to effective judicial remedy against the decision of a supervisory authority or against the data controller or processor, regardless of whether the data controller or processor is a public or private entity.[399] As can be seen from the CJEU's ruling in "Schrems I" and "Schrems II", this existence of an effective administrative and judicial remedy is a crucial criterion for assessing the adequacy of the level of data protection in a third country.

The Cybersecurity Law contains an array of administrative sanctions in case of violation of the provisions concerning to the protection of personal data.[400] It has also provided that whoever violates the provisions of the Cybersecurity Law and causes damages to other people, shall bear civil liabilities. When such violation simultaneously constitutes a violation to the public order, the infringer will be punished in accordance with public order regulations; if it constitutes a crime, criminal liabilities will be borne.[401]

As regards the administrative sanctions, Art. 64 of the Cybersecurity Law merely states that if the network operator or provider of network products or services violate the

[398] Art. 77, GDPR.
[399] Art. 78 and 79, GDPR.
[400] Art. 64, Cybersecurity Law.
[401] Art. 74, Cybersecurity Law.

provisions related to the protection of personal data, the competent department may, alternatively or cumulatively, order it to take corrective action, give it a warning, confiscate its illegal income and/or impose a fine.[402] Depending on the severity of the violation, the competent department could also order the network operator to suspend business operation, close down the website or revoke the business permit or license.[403] However, it is not elaborated whether a natural person who considers its legally protected interests infringed by a network operator is entitled to lodge a complaint to the competent department and requests it to conduct an investigation. It is further not clarified how to decide which authority is the "competent department" in a specific case, and whether the competent department, if it is correctly identified by the data subject at all, must respond to the complaint of the data subject within a certain period of time. In other words, this provision does not by itself grant the data subject a right to effective administrative remedy, instead, it only specifies the type of administrative liabilities an infringer might face when a violation is affirmed by the competent department.

In terms of the judicial remedy, since the protection of personal data is now introduced into the Civil Code, if a data subject considers its legally protected interests infringed by a private network operator, it may bring a civil law proceeding to the court revoking the relevant provisions discussed in the previous part under the Civil Code. According to a case study conducted by the author elsewhere,[404] there were a large number of cases brought by the natural persons to the court relating to their personal data. The majority of these cases were, nevertheless, not brought up based on the protection of personal data, but on other rights established by the then effective General Provisions of the Civil Law,[405] such as the right to privacy, the right to reputation etc. This is not surprising, since the Civil Code has only become effective shortly and the earlier issued General Provisions of the Civil Code effective since 1 October 2017 was too abstract to provide effective protection of personal data. If the network operator is a public authority that processes personal data in a non-administrative act, the data subject may also initiate a civil proceeding against the public authority.[406] If, however, the public

[402] Art. 64, Cybersecurity Law.
[403] Ibid.
[404] YU, Lu; AHL, Bjorn, China's Evolving Data Protection Law and the Financial Credit Information Systen: Court Practice and Suggestions for Legislative Reform. Hong Kong Law Journal, 2021, Vol. 51, p. 19, available at https://ssrn.com/abstract=3782392.
[405] The General Provisions of the Civil Law is outdated by the new Civil Code which became effective on 01.01.2021.
[406] CHENG, Xiao (程啸), On the Nature of Personal Information Rights and Interests in the Civil Code (论我国民

authority processes personal data in or related to an administrative act, and the data subject considers his or her legally protected interest on personal data infringed by the public authority, the data subject could file an administrative case against the public authority.[407]

In terms of the judicial remedy against the decision of a data protection supervisory authority, the Cybersecurity Law does not state whether the data subject can resort to judicial remedies against an omission or decision of the competent department. Though the competent department for the matters concerning data protection is not specified, this competent department under the Cybersecurity Law will in any case be an administrative authority, it would thus be helpful to have a look to the Administrative Procedural Law of the People's Republic of China ("Administrative Procedural Law"), which generally regulates the proceedings brought up by citizens against administrative authorities. Art. 12 of the Administrative Procedural Law stipulates the scope of cases that the courts should accept for an administrative proceeding. It provides in section (6) that, the people's court shall accept "a complaint against an administrative authority's refusal to perform, or failure to respond to an application for the administrative authority to perform, its statutory duties and responsibilities in respect of protecting personal rights, property rights, and other lawful rights and interests",[408] and in section (12) "a complaint claiming that an administrative authority has otherwise infringed upon personal rights, property rights, or other lawful rights and interests".[409] Under the Cybersecurity Law, on the one side, since the data subject does not have an explicit right to lodge a complaint to the competent department, it is not clear whether the competent department has a statutory duty to protect the personal data of the natural persons. And if yes, which department is the "competent" department. On the other side, if a decision is made by the competent department *ex officio* against a network operator due to illegal personal data processing activities, the involved natural person should be able to revoke Art. 12 section (12) and Art. 25[410] to file a suit against the competent department who made the decision. In the judicial practice, there are already cases in

---

法典中个人信息权益的性质), Political Science and Law (政治与法律), 2020, Vol. 8, P. 6.

[407] Ibid.

[408] Art. 12 section (6), Administrative Procedural Law of the People's Republic of China.

[409] Art. 12 section (12), Administrative Procedural Law of the People's Republic of China.

[410] Art. 25 of the Administrative Procedural Law of the People's Republic of China: A person subjected to an administrative action or any other person which is a citizen, a legal person, or any other organization with an interest in the administrative action shall have the right to file a complaint against the administrative action.

that regard.[411]

3. Data protection in consumer law

Another law field that deals with personal data protection in China is the consumer law. The Chinese consumer law, officially known as "Law of the People's Republic of China on Protecting Consumers' Rights and Interests" (hereinafter the "Consumer Protection Law"), was last amended on 25. October 2013 and became effective on 15. March 2014.[412] One of the highlights of this revision was that, a series of new provisions relating to the protection of personal data were introduced to the amended Consumer Protection Law, giving it a consumer data protection character.

3.1 Rules with regard to the protection of consumer personal data

Generally speaking, the introduction of personal data protection mechanism in the amended Consumer Protection Law is achieved systematically via four provisions: first, a right of the consumer to protection of personal data is newly introduced, in addition to the original right to human dignity and being respected for their ethnic mores and customs;[413] Second, the amended Consumer Protection Law also imposes a series of new obligations on the business operator, which include, to comply with the basic data processing principles, to not illegally disclose or sell the collected personal data of the consumer to any third party, to take technical and other necessary measures to secure data safety, as well as to not send business information (advertisement) to the consumer without the latter's prior consent or if the consumer has explicitly rejected to such business information;[414] Further, in terms of the liability of the business operator, the amended Consumer Protection Law specifies that if the business operator infringes the right of the consumer to protection of personal data, he/her shall first and foremost

[411] For example, Guangdong Higher People's Court, Yu Bingwen Financial Administration Case, Second-instance Administrative Ruling, May 19, 2017.
[412] Full text available at http://www.gov.cn/jrzg/2013-10/25/content_2515455.htm.
[413] Art. 14 of the Consumer Protection Law: "In purchasing and using commodities or receiving services, consumers shall be entitled to human dignity, respect for their ethnic mores and customs, and legal protection of personal information".
[414] Art. 29, Consumer Protection Law.

assume civil liabilities, which includes, to cease the infringement, to restore the consumer's reputation, to eliminate the adverse effects, to make apologies and to compensate the consumer for losses.[415] Last, according to Art. 56, in such cases the business operator will also have to expect certain administrative liabilities, such as a fine up to ten times of the illegal income, or, if there is no illegal income, a fine of no more than 500,000 RMB.

In comparison to the Cybersecurity Law, the Consumer Protection Law only protects consumer's personal data. Although everyone is consumer at a certain time, however, if an employee's personal data are misused, he or she obviously cannot invoke the Consumer Protection Law for remedy.

In addition, due to the special aim of the Consumer Protection Law to protect the rights and interests of the consumer in order to ultimately accelerate the development of the consumption and the economy,[416] the protection of personal data in Consumer Protection Law inevitably serves as a consumption stimulation tool, which differs from the basic value of the fundamental rights approach.

3.2 Supervisory authority for the consumer data protection

The competent authority for consumer protection under the Consumer Protection Law is the "Administrative Department for Industry and Commerce and other relevant administrative departments"[417], so should the competent authority for personal data protection within the framework of the Consumer Protection Law be the same.

In terms of the concrete function and power of the said authority, the Consumer Protection Law states that "the relevant administrative departments shall hear the opinions of consumers, consumer associations, and other organizations on issues concerning the transactions of business operators and the quality of commodities and services, and investigate and address such issues in a timely manner." This indicates that the Administrative Department for Industry and Commerce and other relevant

[415] Art. 50, Consumer Protection Law.
[416] Art. 1, Consumer Protection Law.
[417] Art. 32, Consumer Protection Law.

administrative departments are entitled to conduct investigation and make punishment decisions according to the investigation result. In fact, a large amount of local administrative department for industry and commerce have made use of this competence, such as, the Guangxi Administrative Department for Industry and Commerce has published on its official website the 10 most influential cases related to the infringement of consumer rights in 2017, one of which involves unauthorized advertisement using consumers' personal information.[418]

Besides, the consumer could also file a lawsuit with the court if his or her personal data is collected unlawfully or misused by the business operator.[419]

4. Data protection in criminal law

For severe infringements of personal data, such as selling or providing personal data in violation of the relevant laws and regulations, or illegally obtaining personal data for example by stealing, the Chinese criminal law has established a special crime called "the crime of infringing citizen's personal data". The constitutive elements of this crime are specified in Art. 253 (1), which was first introduced in 2009 and amended in 2015.

The criminal law only regulates the sale or provision of personal data in violation of the relevant provisions of the state or the illegal obtainment of personal data in severe circumstances. According to the "Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Infringing on Citizens' Personal Information" ("Interpretation on Infringing on Citizens' Personal Data")[420] severe circumstances are presented in the event of:[421]

"(1) Selling or providing the information on the citizen's whereabouts which is used

[418] Details of the case available at http://www.cicn.com.cn/zggsb/2018-05/03/cms106563article.shtml, last visited on 20.04.2021.
[419] Art. 35, Consumer Protection Law.
[420] Supreme People's Court and the Supreme People's Procuratorate, Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringement of Citizens' Personal Information, Available at http://www.court.gov.cn/fabu-xiangqing-43942.html.
[421] Ibid, Art. 5.

by any other person for committing a crime;

(2) Selling or providing the citizen's personal information to any other person when it or he knows or should have known that the other person uses such information to commit a crime;

(3) Illegally obtaining, selling or providing more than 50 pieces of information on the citizen's whereabouts, communication contents, credit investigation information and property information;

(4) Illegally obtaining, selling or providing more than 500 pieces of accommodation information, communication records, health and physiological information, transaction information and other personal information of the citizen that may affect his or her personal or property safety.

(5) Illegally obtaining, selling or providing more than 5,000 personal information of the citizen other than that as prescribed in items (3) and (4)

……"

In the above-described cases, the person who committed the crime could be sentenced to imprisonment of no more than three years or criminal detention in addition to a fine, or if the circumstances are very serious, be sentenced to imprisonment of no less than three years but not more than seven years in addition to a fine.[422]

The fact that there is no specific single law dealing with the protection of personal data, and that the protection of personal data in the Civil Code and Cybersecurity Law keeps being abstract and controversial, has led to concerns.[423] Since Art. 253 (1) explicitly requires that only the sale or provision of personal data "violating the relevant provisions of the state" and "illegal" obtainment of personal data will be punished by the criminal law, logically, it is necessary that there are relevant provisions in the

[422] Art. 35 (1), Criminal Law.

[423] For example, CAI, Jun (蔡军), Analysis of the Legislation of the Crime of Infringing Personal Information - on the reflection and prospect of the crime legislation（侵犯个人信息犯罪立法的理性分析—兼论对该罪立法的反思与展）, Modern Law Science (现代法学), 2010, Vol. 32, p. 105-112; LIU, Xianquan (刘宪权), FANG, Jinye (方晋晔), Legislation and Perfection of Criminal Law Protection of Personal Information Right (个人信息权刑法保护的立法及完善), Journal of East China University of Political Science and Law (华东政法大学学报), 2009, No. 3, p. 120-130.

Chinese law system regulating the processing of personal data other than the criminal law, otherwise Art. 253 (1) will be useless. It is not to deny that the Civil Code already made a big progress by recognizing the protection of personal data, the Cybersecurity Law, the Consumer Protection Law and numerous other laws and regulations in other area also contain provisions regulating the processing of personal data, but they are scattered, vague and sometimes contradictive.[424] Thus, the criminalization of the illegal obtainment and misuse of personal data actually pushes the legislator to complete and improve the personal data regulation in other areas, so that it won't be the case that the infringement is only criminal punishable, the sufferer can however not claim civil compensations.[425]

In conclusion, the criminal liability for illegal obtainment, sale or provision of personal data may be an effective way to fight against severe crimes, which is also the primary goal of the introduction of such crime into the criminal law, it is however not a solution for a comprehensive protection of the natural persons against the massive data processing conducted by companies and public authorities in the daily life, since most of these processing activities are not "serious or severe" enough to come into the sight of the criminal law, however, they are step by step swallowing people's data privacy.

5. The Personal Information Protection Law

After a comprehensive data protection law was put on the legislation agenda in 2018, on 13 October 2020, the first draft of the PIPL was published by the Standing Committee of the National Congress for public consultation. Later on, on 29 April 2021, the Standing Committee of the National Congress published the second draft of the PIPL for further public consultation. Finally, the official PIPL was passed on 20 August 2021, the law came into force on 1 November 2021.[426]

---

[424] For example, according to the Cybersecurity Law, processing of personal data must all be consented by the related data subject, however, the newest Draft Specification specifies some exceptional circumstances, where the processing of personal data is allowed without the consent of the data subject.

[425] CAI, Jun (蔡军), Analysis of the Legislation of the Crime of Infringing Personal Information - on the reflection and prospect of the crime legislation（侵犯个人信息犯罪立法的理性分析—兼论对该罪立法的反思与展）, Modern Law Science (现代法学), 2010, Vol. 32, p. 105-112.

[426] Available under http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml., last visited on 05.20.2022.

The PIPL has in total 8 chapters, 74 provisions, regulating data processing activities both by private entities and public authorities. Compared to the above analysed scattered rules contained in different laws, the PIPL shows more consistency and provides more legal certainty as a binding law issued by the highest legislative body. However, as will be demonstrated below, the PIPL leaves some of the currently identified problems untouched.

5.1 Data processing principles, rights of the data subjects and obligations of the data controllers

The principles already laid down in the Civil Code and the Cybersecurity Law (including the Specification) are further adopted by the PIPL. These include the principle of lawfulness and fairness, purpose limitation, data minimization, transparency, accuracy and accountability.[427] The contents of these principles are very similar to that of the GDPR. Further, the PIPL also lays down the joint liability of the joint-controllers, the requirement to clarify the rights and obligations of each party in an agreement when the data controller engages a data processing to processor personal data on behalf of him/her, and stricter conditions for the processing of sensitive personal data.

According to the PIPL, the data subject has a right to information, a right to access (review and copy), a right to rectification and supplementation, a right to deletion, and a right to explanation (in terms of the processing rules of the data controller) against the data controller.[428] If an automated decision is made based on personal data, the data subject has a right to explanation and objection to a solely automated decision, provided that the automated decision has a significant impact on the rights or interests of the data subject.[429]

Correspondingly, the data controller must take organizational measures such as adopting internal management procedure, restricting access to the personal data and

[427] Art. 5 to Art. 8, PIPL.
[428] Art. 44 to Art. 48, PIPL
[429] Art. 24, PIPL.

drafting emergency plans, as well as technical measures such as encryption and pseudonymization, in order to ensure compliance with the PIPL.[430] If the amount of the processed personal data goes beyond the standard set by the National Cyberspace Administration, the data controller must designate a data protection officer responsible for the internal supervision of the protective measures.[431] Further, the data controller should have their compliance measures audited, and conduct a risk assessment in certain circumstances, such as processing sensitive data, using personal data for automated decision etc.[432] In case of a data leakage, the data controller must inform the supervisory authority and the involved natural person.[433] If a data controller is located in a third country, it has to designate a representative in China and report the information of the representative to the supervisory authority.[434]

It can be observed that the material rights and obligations on paper are generally comparable to that of the GDPR. Even though differences still exist, for example, the legal bases provided in the PIPL are not exactly the same as those contained in the GDPR, these fine differences do not significantly reduce the level of data protection in China, since the most majority of the material principles and rights of the data subjects guaranteed in the GDPR are reflected in the PIPL. Besides, according to the ruling of the CJEU in "Schrems I", the adequacy assessment under the GDPR merely requires the level of protection in a third country to be "essentially equivalent" to that of the EU,[435] an identical or point-to-point replication of the rules in the GDPR is not required.[436] More important is the effective implementation, supervision and enforcement of these material rules.[437]

5.2 The regulation of data processing activities carried out by public authorities

The PIPL explicitly declares in Art. 33 its applicability to the data processing activities

[430] Art. 51, PIPL
[431] Art. 52, PIPL.
[432] Art. 55 and Art. 56, PIPL.
[433] Art. 57, PIPL.
[434] Art. 53, PIPL.
[435] CJEU, C-362/14, 06.10.2015, para. 73.
[436] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, para. 3.
[437] Ibid.

by public authorities. The processing principles, right of the data subjects and obligations of the data controllers in the general part apply to the public authorities. Worth noting is that in addition to the general rules applicable to all kinds of data controllers, a section under the chapter II "Rules for processing of personal data" is specifically contributed to the data processing activities by public authorities (section 3). The rules of this specific section prevail other general rules. This section has 5 provisions and will be further elaborated on below.

5.2.1. Legal basis for data processing by public authorities

According to Art. 13 (3) PIPL, data controllers may process personal data if the data processing is "necessary for the performance of a statutory duty or obligation", which could provide the public authorities with a lawful way to process personal data. However, it must be noted that, similar to Art. 6 section 1 (e) GDPR, strictly speaking, this provision is only a gateway for specific laws to set out legal bases for processing personal data.[438] Not Art. 13 (3) PIPL, but the relevant specific duties or obligations laid down in specific laws are the legal bases for the data processing.

Unfortunately, unlike the GDPR, the PIPL does not provide for further conditions for the specific laws that set out such statutory duty or obligation. Under the GDPR, Art. 6 section 3 requires that the legal basis for data processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority must be laid down by Union law or Member State law, and the purpose of the processing shall be necessary for performing the public task or exercising the official authority.[439] Further, the Union or the Member state law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.[440] The requirement of "necessity", "objective of public interest" and "proportionate" plays a crucial role here, since the "Union law or Member State law" does not only refer to laws that are enacted by the legislative body, but also administrative regulations or even municipal codes or

[438] See BUCHNER, Benedikt; PETRI, Thomas, Art. 6, in: KÜHLING, Jürgen; BUCHNER, Benedik, GDPR – Federal Data Protection Law (DS-GVO/BDSG), C.H. BECK, 3rd Edition, 2020, p. 83.
[439] Art. 6, section 3, GDPR.
[440] Ibid.

collective agreement,[441] which could be issued by public authorities themselves and did not go through legislation procedures as strict as parliamentary laws. Besides, even parliamentary law might fail to meet these requirements. It is not rare that a law permitting or obliging public authorities to process personal data are considered "disproportionate" by the CJEU. For example, the CJEU has made clear in the Bara case,[442] the Schecke case,[443] the Digital Rights Ireland case[444] and the Tele2 case [445] that EU laws or nationals entaining obligations that interfere with the fundamental rights to the protection of personal data should be limited to what is strict necessary and be proportionate to the objective it pursued in the light of Articles 7, 8 and 52 of the Charter of Fundamental Rights of the European Union, otherwise the questioned rules are invalid and the data processing relied upon on such rules are unlawful. By this way, the EU has a review mechanism in place which prevents the legislative or executive body from making laws that allow excessive data processing.

Such requirement and review mechanism is, however, missing in the PIPL and generally in the Chinese data protection law system. Even though the PIPL embodies the general principles of necessity and data minimisation, these general principles naturally face difficulties of being applied in the practice. This is especially the case, when there is a law or administrative regulation allowing public authorities to process personal data massively. Thus, the general principles laid down in the PIPL could not fill this gap.

More importantly, there is no judicial review of legislative acts in China. Courts may only review specific acts of the public authorities, not administrative regulations or rules that are binding to the general public.[446] However, there is indeed law review carried out by legislative and executive body. According to the Legislation Law of the People's Republic of China, when a law with lower hierarchy violates another law with higher hierarchy, or a departmental or local regulation contains rules that are deemed impropriate, the People's Congress or its Standing Committee are entitled to amend or

[441] Recital 41, GDPR; see also BUCHNER, Benedikt; PETRI, Thomas, Art. 6, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR – Federal Data Protection Law (DS-GVO/BDSG), C.H. BECK, 3rd Edition, 2020, p. 84.
[442] CJEU, C-201/14, 01.10.2015.
[443] CJEU, joined cases C-92/09 and C-93/09, 09.11.2010.
[444] CJEU, joined cases C-293/12 and C-594/12, 08.04.2014.
[445] CJEU, C-203/15, 21.12.2016.
[446] Art. 13, Administrative Procedural Law of the People's Republic of China of the People's Republic of China.

invalidate the law, and the State Council is entitled to amend or invalidate the departmental or local governmental regulation.[447] Nevertheless, since there is no explicit right to the protection of personal data in the Chinese Constitution, not to mention that the requirement of "proportionate" regarding the laws or administrative regulations interfering with the fundamental right to the protection of personal data, there is no legal grounds for the People's Congress or its Standing Committee to review the laws that containing such interference. Besides, it is skeptical whether a mechanism of self-review by the People's Congress and its Standing Committee and an administrative system-inside review by the State Council is effective. At least there has been no precedent for invalidating a law or administrative regulation due to disproportionate interference with the right of data protection so far.

5.2.2. Data access by intelligence and law enforcement authorities

Since public authorities referred to in the PIPL cover all state authorities and organizations invested with public functions by laws or administrative regulations without mentioning any exceptions, it also includes intelligence services and law enforcement authorities. This means, the above-mentioned legal basis and other provisions of the PIPL apply to the intelligence services and law enforcement authorities too. As previously noted, now that the data access by public authorities, in particular within the framework of surveillance programs, has been the main reason of the annulment of the "Safe Harbour" and the "Privacy Shield" by the CJEU, it should be assessed in the light of the "Schrems I" and "Schrems II" judgement whether these general rules governing the data access by public authorities in the PIPL could actually meet the threshold set out by the CJEU. In that regard, the CJEU has made clear in "Schrems II" the requirements for limitations on the fundamental rights. The CJEU first acknowledged that fundamental rights are not absolute rights, they must be considered in relation to their function in society.[448] However, the interference with or limitation on the fundamental rights must respect the essence of those fundamental rights. Specifically, first of all, limitation on fundamental rights must be provided in law, which

[447] Art. 96 and 97, Legislation Law of the People's Republic of China.
[448] CJEU, C-311/18, 16.07.2020, para. 172.

more specifically means, in the word of the CJEU, that the legal basis which permits the interference must itself define the scope of the limitation.[449] Besides, the limitations are subject to the principle of proportionality, which means the limitations must be strict necessary.[450] To that end, the CJEU further required that "*the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards…it must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is necessary*". [451]

As regard the PIPL, as stated above, the PIPL provides "data processing necessary for the performance of a statutory duty or obligation" as legal basis for the data processing by intelligence and law enforcement authorities. In addition, Art. 34 states that, in the event public authorities need to process personal data for the purpose of performing a statutory duty, they should only do this in accordance with the prescribed competences and procedures laid down in the laws and administrative regulations. The scope and extent of such processing must not exceed what is necessary for the performance of that statutory authority. In the light of the CJEU's ruling in "Schrems I" and "Schrems II" as analyzed above, it is apparent that these two provisions by themselves provide neither a specific legal basis nor precise rules or requirements regarding the scope and conditions of the data processing by intelligence and law enforcement authorities. In other words, the provisions in the PIPL concerning data processing by public authorities are only general framework that basically iterates the requirements set out by the CJEU in "Schrems I" and "Schrems II" – instead of implementing them. It must thus be concluded that the PIPL itself does not satisfy the requirements set out by the CJEU for limitations on the fundamental rights. Rather, the specific law that confers the statutory duty on the intelligence and law enforcement authorities – whereby also grants them the legal basis to access personal data for it – must be scrutinized. Only on that basis it can be assessed whether the specific legal basis is provided for by law and meets the principle or proportionality. Such scrutiny and assessment will be made in a later

[449] Ibid, para. 174.
[450] Ibid.
[451] Ibid, para. 176.

section.

5.3 Supervision and enforcement

5.3.1 Designation of the supervisory authority and independent status

The existence of an independent supervisory authority with the powers to monitor and enforce the material data protection rules is crucial for the assessment of an adequate level of data protection in the practice.[452] In "Schrems II", the CJEU has denied the independence status of the Ombudsperson mechanism, since it appointed by the US State Department and can be dismissed or revoked by it anytime, thus is not free from the executive.[453] In order to obtain an independent status, the supervisory authority must refrain from any activities incompatible with its duties under the data protection law.[454] It should have its own staff chosen by itself or an independent body, as well as a separate budget to be financially independent from outside pressures.[455]

In terms of the competent authority responsible for the supervision of data protection compliance, the PIPL has followed the approach under the Cybersecurity Law. It states that the relevant departments of the State Council are responsible for the data protection implementation, supervision and administration within their own competences, and the State Cyberspace Administration shall coordinate the data protection implementation, supervision and administration.[456] Further, the competences of the data protection supervisory authority on the local level should be determined in accordance with the relevant rules and regulations of the State.[457] Thus, the supervisory authority is not unambiguously designated in the PIPL. Rather, the competent supervision authority must be individually determined in each case, which is not always easy for a natural person, since the "relevant departments" and their "competences" are not straightforward to figure out. Thus, it must be assessed that the data protection

[452] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, para. 95.
[453] CJEU, C-311/18, 16.07.2020, para. 195.
[454] Recital 121, GDPR.
[455] Recital 120 and 121, GDPR.
[456] Art. 60, PIPL.
[457] Ibid.

supervisory authority is still not designated with sufficient legal certainty under the PIPL.

In addition, because the supervisory authorities for the data protection compliance are the "relevant departments" that may oversee the business and operation of the data controller generally, there is no guarantee that these "relevant departments" will retreat from activities that are incompatible with their duty to supervise the data controller's compliance with the data protection rules. It is not clear either, whether these relevant departments shall have separate personnel and independent financial resources to ensure their independent status. Thus, in the light of the "Schrems II" judgement, these "relevant departments" are in no means independent from the executive, neither organizational nor operational. From all the above analyzed, it must be ascertained that the supervisory authorities, when identifiable in the individual case at all, rather do not show an independent status in terms of their duty to supervise the compliance with data protection rules.

5.3.2 Tasks and powers of the supervisory authority

The PIPL imposes an array of tasks on the supervisory authorities. The supervisory authorities should promote public awareness of data protection, guide and supervise the compliance of the data controllers, accept and handle complaints and reports related to data protection, investigate and punish illegal data processing activities as well as other duties and tasks prescribed in laws and administrative regulations.[458]

The supervisory authorities have corrective and investigative powers to help them fulfill the tasks stated above. They may inquire the involved parties and investigate the facts and circumstances related to the data processing; require access to and copy the documents concerning the data processing; conduct on-site inspections, investigate into suspected illegal processing; inspect the equipment and objects concerning to the data processing, seize and detain them in the presence of proof.[459] Further, if the supervisory authorities identified risks in the processing, they could also bring it to the legal

[458] Art. 61, PIPL.
[459] Art. 63, PIPL.

representative or the data protection officer and require them to make corrections to eliminate the risks.[460] Moreover, if a data controller processes personal data against the rules laid down in the PIPL, or does not take necessary security measures to protect personal data, the supervisory authorities may order correction, confiscate the illegal income, issue a warning. If the data controller fails or refuses to make corrections, the supervisory authorities may further issue a fine up to one million RMB against the data controller, and a fine between ten thousand and hundred thousand RMB against the direct responsible person(s).[461] In severe circumstances, the monetary fine against the data controller may be lifted up to 50 million RMB or 5% of the business turnover in the previous year.[462]

With these tasks and powers, the supervisory authorities should have the necessary means to monitor and enforce the compliance with the data protection rules. As demonstrated above, the problem lies rather in the determination of the competent supervisory authority and its independent exercise of these tasks and powers.

5.4 Remedies and liabilities

5.4.1 Administrative remedy

The natural persons should have effective administrative and judicial remedies to enforce their rights effectively. Compared to the Cybersecurity Law that does not explicitly grants the involved natural person a right to lodge a complaint, the PIPL provides that any organization and natural person has a right to lodge a complaint against illegal data processing to the supervisory authorities. The supervisory authorities should handle the complaint in a timely manner, and inform the complainant of the result. The supervisory authorities should also publish the contact information for accepting complaints.[463] Under the current stand, authorities such as the State Administration for Market Regulation, Ministry of Industry and Information, Ministry of Public Security inclusive their local branches have all dealt with complaints lodged

[460] Art. 64, PIPL.
[461] Art. 66, PIPL.
[462] Ibid.
[463] Art. 65, PIPL.

by natural persons with regard to the protection of personal data. Also, the Consumer Protection Association with its numerous local centers accept data protection related complaints arising from the consumption area.[464] An example hereof is, due to the popularity of Apps and their massive collection of personal data, the State Cyberspace Administration, the Ministry of Industry and Information, the Ministry of Public Security and the State Administration for Market Regulation have established a special working group for a campaign against unlawful data processing by Apps.[465] Under this special campaign, an official Wechat account is opened to receive complaints and publish investigation results. Since Wechat is used in China almost by every Smart-phone user, this is considered a convenient way to encourage people to lodge complaints.

5.4.2 Judicial remedies under civil law

The PIPL itself does not expressly grant data subjects any judicial remedy. It only stated that the data controller has to bear tort liabilities when a natural person's right and interest on its personal data is infringed and the data controller could not prove that it has no fault.

However, the general framework of the civil law should be able to compensate this loophole indirectly. In the event of a private person or organization violates against the provisions of the PIPL, the involved natural person may file a civil law proceeding to the court based on the PIPL and the relevant provisions concerning data protection in the Civil Code. Art. 995 of the Civil Code states that the person whose personality rights is infringed may claim civil liabilities against the infringer, including monetary compensation as well as injunctive relief, removal of obstacles, elimination of danger, elimination of adverse effects, rehabilitation of reputation, or extending a formal apology.[466] Since the protection of personal data should be a legally protected personality interest under the Civil Code, the legal liability resulted from its

[464] Consumer Protection Association of Shanxi, "Leakage of Personal Information Mediated by the Consumer Protection Association", 7 May 2019.
[465] The State Cyberspace Administration, the Ministry of Industry and Information, the Ministry of Public Security and the State Administration for Market Regulation, "Ways to Determine Unlawful Data Processing by Apps", 28.11.2019.
[466] Art. 995, Civil Code.

infringement is regulated in Book 7 “Tort Liability”.

In this regard, it is crucial to prove that the necessary constructive elements for the tort liability caused by the infringement are fulfilled. Since the constructive elements for the tort liability caused by the infringement of personal data is not directly provided for in the provisions relating to the protection of personal data, one can only refer to the general rules laid down in Book 7 of the Civil Code. Art. 1165 in Book 7 provides that “A person who infringes upon a civil right or interest of another person at fault and causes harm to him or her, shall be subject to tort liability. If, according to the law, a person is presumed to have fault on the infringement and the person could not approve against it, the person shall be subject to tort liability”.[467] The liability of the data controller under the PIPL falls under the second case. Namely, Art. 69 sets out that where the data processing activities of the data controller infringe the rights and interests of the data subject regarding to their personal data and causes damage to him/her, and the data controller cannot prove that it is not at fault, it shall bear the tort liability for the caused damages. This means, the PIPL adopts the approach of “presumption of fault”. In addition, the natural person also has to approve that the data controller has committed the infringement (infringing act), the existence of damage and the causality between the infringing act and the damage.[468] The damages can be both material or immaterial.[469]

The GDPR also contains a specific legal basis for claiming compensation and civil liabilities. According to Art. 82 section 1 GDPR, the constructive elements for claiming for compensation are a) an infringement of the GDPR; b) the data subject has suffered material or non-material damages; c) there is a causality between the infringement and the damages.[470] This seems to indicate that a “fault” of the data controller or processor is unnecessary and irrelevant, thus establishing a strict responsibility.[471] However, Art.

---

[467] Art. 1165, Civil Code.

[468] ZHU, Xuanye (朱宣烨), Research on the Path of Civil Protection of Personal Information in the New Era - From the Perspective of the Distribution of Responsibilities in the Presence of Third-Party Information Processors (新时代个人信息民事保护路径研究-以存在第三方信息处理者情况下的责任分配为视角), Legal Science Magazine (法学杂志), 2018, Vol. 39, No. 11, p. 133-140.

[469] Art. 1183, Civil Code.

[470] Art. 82 section 1, GDPR.

[471] To this opinion: FRENZEL, Eike Michael, Art. 82, in: PAAL, Boris P.; PAULY, Daniel A., GDPR – Federal Data Protection Act (DS-GVO – BDSG), 2nd Edition, 2018, p. 6; GEISSLER, Dennis; STRÖBEL, Lukas, Claims for Damages Under Data Protection Law in the Model Determination Procedure (Datenschutzrechtliche Schadensersatzansprüche im Musterfeststellungsverfahren), NJW 2019, No. 47, p. 3414.

82 section 3 GDPR provides an exemption for the liability if the data controller or processor could approve that *"it is not in any way responsible for the event giving rise to the damage*".[472] Based on this, some scholars hold the opinion that the liability under Art. 82 is built on a presumption of fault that the data controller or processor has to approve against it to exempt from liability.[473] In this sense, the GDPR and the PIPL take the same approach. In terms of the extent to which the infringement act, damage and causality can be proved, it is not to exclude that fine differences exist in the two legal systems, however, these differences could also exist in the Member States of the EU.[474] These differences should not constitute a substantial argument against the existence of an effective judicial remedy under the Civil Code and the PIPL in China.

5.4.3 Judicial remedy under administrative law

The PIPL does not provide whether the data subject has a right to judicial remedy against the public authorities as data controller or the decision of the data protection supervisory authority. One must again resort to the more general administrative law. If an administrative authority violates the data protection rules in the course of or related to an administrative act, or a natural person is not satisfied with a decision made by a supervisory authority, the natural person may file an administrative proceeding against the public authority/supervisory authority based on Art. 12 section (6) and section (12) Administrative Procedural Law, as demonstrated above in the part judicial remedies under the Cybersecurity Law. Since it is now explicitly stipulated in the PIPL that the public authority as data controller is subject to the PIPL, and the supervisory authorities are obliged to accept and handle complaints from the natural persons, the barriers noted in the judicial remedies under the Cybersecurity Law should no longer impede the judicial remedy based on the Administrative Procedural Law.

However, it must be noted that obstacles still exist as regards law enforcement authorities such as the police when performing law enforcement duties, the

---

[472] Art. 82 section 3, GDPR.
[473] HÄRTING, Niko, GDPR (Datenschutz-Grundverordnung), Otttoschmidt, 2016, p. 234.
[474] ZANFIR-FORTUNE, Gabriela, Art. 82, in: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher. The EU Data Protection Regulation (GDPR): A Commentary. Oxford University Press, Oxford, 1st Edition 2020, p. 1175.

procuratorate, the courts and the intelligence department etc., since these state organs are not administrative authorities or not carrying out administrative acts. Consequently, the data subject cannot seek judicial remedy based on the Administrative Procedural Law. Another law governing the responsibilities of public authorities is the State Compensation Law.[475] The State Compensation Law grants natural persons and organisations (including citizens of the P.R.C. and foreigners)[476] the right to receive state compensation. However, the compensation scope is only limited to the cases where an administrative authority or its personals commit certain acts infringing upon a person's personal rights (limited to right of freedom, body or life) or property rights,[477] or when a criminal investigation, prosecution or trial organ commit acts infringing upon a person's personal rights (limited to detention, arrest, torture, battery or maltreatment, illegal use of weapon) or property rights[478]. Apparently, the scope of compensation in terms of the infringed rights and infringing subjects is very limited. In the first place, the State Compensation Law does not apply to infringement upon the right or interest to the protection of personal data. Besides, the Law does not grant natural persons a right to receive compensation against the intelligence authorities. In the second place, the right to receive state compensation is not identical to an effective judicial remedy, since compensation is merely one art of responsibility and it is not always what the data subject wants. If, for example, the data subject wishes to have access to the data, to have the data corrected or deleted, the State Compensation Law would not apply.

However, the analysis made above is merely based on the general rules in the PIPL and in the Administrative Procedural Law and in the State Compensation Law. It must be further assessed whether the law specifically concerning these law enforcement authorities and intelligence authorities provide data subjects with the possibility to judicial remedy, this will be analyzed in a later section.

5.5 Brief summary

This section scrutinizes the substantial data protection rules in China. It begins with the

[475] P.R.C. State Compensation Law, adopted on 12 May 1994, most recently amended on 26.10.2012.
[476] Art. 40, State Compensation Law.
[477] Art. 3, State Compensation Law.
[478] Art. 17 and 18, State Compensation Law.

constitutional status of the protection of personal data in China and comes to the conclusion that the protection of personal data as a fundamental right remains a scholar opinion, which leaves it still far away from a recognized fundamental right in the Constitution.

With the recent promulgation of the Civil Code with explicit data protection provisions, the protection of personal data is officially established as a protection of the personality of the natural persons. The introduction of the protection of personal data in the Civil Code provides a legal basis for the data subject to bring up a civil law proceeding against the data controller or processor in case of infringement.

The Cybersecurity Law lays down principles similar to those contained in the GDPR, it also grants the data subject the right to information, the right to rectification for incorrect data and the right to deletion for data that is collected against the law or the agreement between the parties. The Specification as a recommended standard further expands the scope of data processing principles, rights of the data subjects as well as technical and organizational obligations of the data controllers, drawing the Chinese data protection law even closer to the GDPR. The Specification also makes a distinguish between normal personal data and sensitive data, imposing stricter restrictions for the processing of sensitive data. However, in terms of the detailed substantial rules, there are still fine differences that lower the data protection level in China, for instance, the conditions for valid consent. Despite all this, the Cybersecurity Law framework has two crucial flaws that impede its effort to improve the data protection level in China. The first one lies in the unbinding nature of the Specification. The Cybersecurity Law only contain 4 provisions[479] directly related to the data protection principles, the rights of the data subjects and obligations of the data controllers. These provisions are highly abstract, rather declaratory with little guidance value for the practice. The Specification does not only provide practicable guidance for the implementation of the existing rules laid down in the Cybersecurity Law, it actually expands the substantial scope of the GDPR in terms of both the application scope (from "network operator" to "all organizations that process personal data") and the material rules by adopting more processing principles, data subject rights and data controller

[479] Art. 41 to 44, Cybersecurity Law.

obligations. However, since the Specification is a recommended standard that has no binding effect, its impact on the practice is very limited. Another drawback of the Cybersecurity Law framework is the lack of regulation of data processing activities by the public authorities when performing their public functions. Against the background of numerous social governance projects in China, for example the commonly used "face recognition" in major train stations and airports, the Social Credit System that gathers and integrates citizen data for rebuilding trust in the society, the public authorities hold a huge amount of data of the citizens. The Cybersecurity Law's unsophisticated, declaratory data protection rules are not able to provide behavior guidance for the public authorities, in fact, it is doubted that the data protection provisions contained in the Cybersecurity Law are applicable to the public authorities when performing their public functions at all. In addition to the flaws stated above, under the Cybersecurity Law, there is no specific independent authority supervising the implementation of the data protection provisions. Nor is the data subject granted an explicit right to lodge a complaint to the so-called "competent department" that has the competence to order administrative sanctions against the data controller. The judicial remedy against a data controller is theoretically possible under the Civil Code and the Administrative Procedural Law. Problem arises, again, in terms of the public authority as data controller, since it is unclear what kind of rules apply to the public authorities, for example, whether the public authorities need a legal basis to process personal data. Thus, judicial remedies against public authorities as data controllers or supervisory authorities face significant challenges in the practice.

Personal data are also to a certain degree protected in the Chinese consumer law and the criminal law. In comparison to the Cybersecurity Law, the consumer law only protects consumer's personal data. Although everyone is consumer at a certain time, however, if an employee's personal data are misused, he or she obviously cannot invoke the consumer law for remedy. There is no independent data protection supervisory authority in the consumer law either. As regards data protection per criminal law, the criminal liability for illegal obtainment, sale or provision of personal data may be an effective way to fight against severe crimes, it is however not a solution for a comprehensive protection of the natural persons against the massive data processing conducted by companies and public authorities in the daily life, since most of these

processing activities are not “serious or severe” enough to come into the sight of the criminal law.

The newest and a most important data protection law development in China is the promulgation of the PIPL, a comprehensive data protection law. It can be observed from this PIPL that the material rights and obligations on paper are generally comparable to that of the GDPR. The PIPL also explicitly applies to the data processing activities by public authorities, making “data processing necessary for the performance of a statutory duty or obligation” a legitimate way for public authorities to process personal data. In addition, it also requires public authorities to process personal data in accordance with the prescribed competences and procedures laid down in the laws and administrative regulations, and the scope and extent of such processing must not exceed what is necessary for the performance of that statutory authority. There is no doubt about the many positive influences this might bring along, however, in the light of the “Schrems II”, it must be assessed that this general stipulation of legal basis and requirement of necessity by itself is not sufficient for ensuring a level of protection that is essentially equivalent to that is guaranteed within the EU. Instead, one must look into the specific law or administrative regulations providing a legal basis for data processing by public authorities, in order to find out whether such laws or administrative regulations also lay down the scope and application conditions for the data processing, as well as whether such rules meet the principle of proportionality. In the light of “Schrems I” and “Schrems II”, in particular the data access by intelligence and law enforcement authorities must be further scrutinized. Further, in terms of the authority responsible for the supervision of data protection compliance, the PIPL provides that the relevant departments of the State Council are responsible for the data protection implementation, supervision and administration within their own competences, and the State Cyberspace Administration shall coordinate the data protection implementation, supervision and administration. Thus, the PIPL did not lay down a single, special data protection supervisory authority. Rather, the competent supervision authority must be individually determined in each case. In addition, it must be ascertained that the supervisory authorities, when identifiable in the individual case at all, rather do not show an independent status in terms of their duty to supervise the compliance with the PIPL. In this sense, the PIPL has failed to introduce an independent data protection supervisory

authority like that in the GDPR, which makes the practical impact of the substantial rules largely questionable. Lastly, the PIPL does grant the data subject a right to administrative and judicial remedy indirectly in connection with the Civil Code and the Administrative Procedural Law. In the event of violations against the provisions of the PIPL, the data subject may file a civil law proceeding to the court based on the PIPL and the data protection provisions the Civil Code. If an infringement is caused by an administrative authority as data controller processing personal data in the course of or related to an administrative act, or the natural person is not satisfied with a decision made by the supervisory authorities, the natural person may file an administrative proceeding against the public authority/supervisory authority based on the Administrative Procedural Law. However, problems arise when intelligence and law enforcement authorities are involved, since the Administrative Procedural Law only apply to administrative organs and the State Compensation Law does not apply to infringement upon the right or interest on personal data.

III. Access of Personal Data by Public Authorities for Purposes of Law Enforcement and National Security in China

1. General legal framework

As noted previously, the Chinese Constitution contains a special chapter dedicated to the fundamental rights. In terms of the function of the fundamental rights, compared to the nature of the fundamental rights as a strong defense against the state power in some European countries, the Chinese Constitution stresses the consistency between the State, society and citizens.[480] Notwithstanding this, fundamental rights in China still have a certain degree of defense function against the state power.[481] On the one hand, it lies in the inherent nature of the fundamental rights, on the other hand, Art. 33 of the Chinese Constitution explicitly states that "the State respects and preserves human rights", this obligation to respect the human rights (fundamental rights are human rights

[480] HAN, Dayuan (韩大元), The Origin and Evolution of the Concept of Fundamental Rights in China (基本权利概念在中国的起源与演变)，China Legal Science (中国法学)，2009, Vol. 6, p. 23-25.

[481] See ZHANG, Xiang (张翔)，The Defensive Function of Fundamental Rights (论基本权利的防御权功能), Jurist Review (法学家)，2005, Vol. 2, p. 65.

that explicitly recognized by the Constitution) requires the State to restrain from activities that might infringe the fundamental rights of the citizens.[482] However, protection of personal data is not officially recognized as a fundamental right in the Chinese Constitution. In the absence of this constitutional status, the defense of data protection against access and use by public authorities is in lack of a strong legal basis of high-hierarchy.

Though the protection of personal data is not specifically recognized as a fundamental right through the wording or the interpretation of the Chinese Constitution, there are other fundamental rights established in the Constitution that are related to the protection of personal data. The two closest fundamental rights relating to the protection of personal data are Art. 38 that protects the personal dignity of the citizens of the People's Republic of China and Art. 40 that protects the freedom and secrecy of correspondence of citizens of the People's Republic of China. The protection of personality dignity could theoretically be interpreted to contain a fundamental protection of personal data, if done by the organ competent to interpret the Constitution (the National People's Congress and the Standing Committee of the National People's Congress[483]), this is however not yet the case. The protection of freedom and secrecy of correspondence obviously leads to the protection of personal data contained in or related to the correspondence, including electronical correspondence. However, there is an exception that significantly impedes the protection of secrecy of correspondence, namely, to meet the needs of state security or of criminal investigation, the public security authority and the procuratorate are permitted to censor correspondence in accordance with procedures prescribed by law. In fact, this exception has become a legal source for sectoral laws or regulations to grant the public security authority and the procuratorate access to personal data for the purposes of criminal enforcement and national security,[484] without being much restricted since a constitutional review of national laws by a specific constitution court or the supreme court does not exist in China.

[482] Ibid.
[483] Art. 62 and 67, Chinese Constitution.
[484] WANG, Zhizheng, Systematic Government Access to Private-Sector Data in China. International Data Privacy Law, 2012, Vol. 2, No. 4, pp. 220-229.

2. Access by public authorities for criminal law enforcement purposes

As noted above, the access to personal data by public authorities for criminal law enforcement purposes has its primary legal basis in the Constitution and is implemented in the Criminal Procedure Law[485] in more details.

2.1 Compulsory investigation and evidence collection

Art. 48 of the Criminal Procedure Law provides the type of evidences that may be used to prove the facts of a case. Among these evidence types, documentary evidence and electronic data may in particular contain a large amount of personal data.

During a criminal investigation, the public security authorities and prosecutors (together referred to as "Criminal Investigators") may gather evidence either through own investigation measures, such as search and seizure,[486] or with the assistance of third parties by asking the relevant individuals or entities to hand over evidences[487]. In both cases, electronic data is an important type of evidence that more and more often becomes the object of a criminal investigation in the internet era. Given the popularity and specificity of the electronic data as evidence, the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security has jointly issued a "Notice on Several Issues concerning the Collection, Taking, Examination, and Judgment of Electronic Data in the Handling of Criminal Cases" (the "Electronic Data Notice").[488] According to this Electronic Data Notice, electronic data may be collected by seizure of the physical storage medium or remote network access.[489] In contrast to the requirement of obtaining a court warrant for search and seizure in many countries, under the Chinese Criminal Procedure Law, a search and/or seizure may be approved by the head of the public security authority or the procuratorate above the county

[485] Criminal Procedure Law of the People's Republic of China, last amended on 26.10.2018.
[486] Art. 136 and 141, Criminal Procedure Law.
[487] Art. 137, Criminal Procedure Law.
[488] Notice of the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security on Issuing the Provisions on Several Issues concerning the Collection, Taking, Examination, and Judgment of Electronic Data in the Handling of Criminal Cases, issued on 09.09.2016.
[489] Art. 9, Electronic Data Notice.

level.[490] In other words, the search or seizure of electronic data is approved internally within the Criminal Investigators system, not by an independent judge. Even in the case of remote network access, which would usually constitute a hidden technical investigation measure[491] that intervenes the private sphere of the involved natural person even more strongly, the approval is still to be issued by the head of the public security authority above the city level.[492] Further, if the electronic data needs to be handed over from a third party, the "notice to hand over evidences" can be issued even easier, namely by the head of the specific department inside of the public security authority that is responsible for handling the case.[493] This self-authorization inevitably leads to the doubt about the fairness and necessity of the investigation measures and the collection of personal data.

In addition, the scope of the electronic data to be collected is not specified. The provisions concerning the approval for search and seizure do not mention whether the approval should specify the scope of the electronic data, the "notice to hand over evidences" must only provide the relevant information on the electronic data. Based on this vagueness, scholars have criticized that the collection of electronic data will easily lead to over-access to personal data in the practice.[494] In the light of the "Schrems II" judgement, in which the CJEU expressly required that the legal basis allowing the limitation on the fundamental right must at the same time define the scope of such limitation and the limitation must only apply when it is strictly necessary,[495] this lack of specific definition of the scope and control of the collection of electronic data under the Criminal Procedure Law and the Electronic Data Notice could not be assessed as satisfying the requirements set out by the CJEU.

---

[490] Art. 222 and 228, Provisions on the Procedures for Handling Criminal Cases by Public Security Authorities, last amended on 20.07.2020 by the Ministry of Public Security Authority.
[491] Technical investigation measures are measures with strong surveillance nature such as record surveillance, location and activity surveillance, interception of communications, or premise surveillance, Art. 264 of the Provisions on the Procedures for Handling Criminal Cases by Public Security Authorities.
[492] Art. 265, Provisions on the Procedures for Handling Criminal Cases by Public Security Authorities.
[493] Art. 62, Provisions on the Procedures for Handling Criminal Cases by Public Security Authorities.
[494] JIANG, Yong (蒋勇), The Procedural Law Change of China's Electronic Evidence Collection Rules From the Perspective of Personal Information Protection (个人信息保护视野下中国电子取证规则的程序法转向), Journal of Xi'an Jiaotong University (西安交通大学学报)，2019, Vol. 39, No. 6, p. 144; LI, Liang (李亮), Inspection and Exploration of Personal Information Protection in the New Criminal Procedure Law (新刑事诉讼法中个人信息保护的检视与路径探索), Humanities & Social Sciences Journal of Hainan University (海南大学学报人文社会科学版), 2014, No. 2, p. 93-94.
[495] CJEU, C-311/18, 16.07.2020, para.175-176.

2.2 Supervision of the compulsory investigation and collection of electronic data

The Criminal Procedure Law provides two possibilities to supervise the investigation measures and the collection of evidence by the Criminal Investigators. First, the concerned person or his/her representative may file a petition with the handling criminal investigation authority (the public security authority or the procuratorate), if the personnel of the said criminal investigation authority seize any property that is irrelevant to the case or refuses to terminate the seize after it becomes unnecessary.[496] Against the decision resulted from such petition, the concerned person or his/her representative may file an appeal with the procuratorate at the same level, if the original handling criminal investigation authority is the public security authority; or, if the case is directly investigated by the procuratorate, the concerned person may file an appeal with the procuratorate at the next higher level.[497] Obviously, this kind of supervision still takes place within the criminal investigation authorities, thus it is in no way independent. Besides, according to the above, the concerned person or its representative only has a right to file a petition or appeal if the seized good is not or no more relevant to the case, however, in most cases, some data in the seized good, for example in a cellphone, are related to the case, while some others are not. It is not clear how such cases should be handled. More importantly, it is not clear whether the above rules should apply, when there is no physical storage medium for the personal data at all, such as when the electronic data are obtained by means of remote network access, since strictly speaking, such data are not the "property" of the involved party.

The second possibility to challenge the evidence collection activities of the criminal investigation authority can be found in Art. 56-60 of the Criminal Procedure Law. According to Art. 56 of the Criminal Procedure Law, the court should examine whether the evidences presented by the Criminal Investigators are obtained by illegal means, illegally obtained evidences should be excluded from the evidence list. However, this option also shows several flaws. First, the examination and exclusion of illegally obtained evidence is only applicable to physical evidence and documentary evidence,

[496] Art. 117, Criminal Procedure Law.
[497] Ibid.

not to electronic evidence.[498] Second, even if it applies to electronic evidence, and it is confirmed that a set of electronic data is illegally obtained, the result would only be the exclusion of that evidence. Though Art. 57 provides that if a crime is committed during the illegal obtainment of evidence, the procuratorate shall investigate it in accordance with the law, the illegal access of personal data by the Criminal Investigators would unlikely constitute a crime, since the standards for a personal data related crime are set very high, as showed in the previous part of this dissertation.

To sum up, the first supervision mechanism takes place within the criminal investigation authorities, thus it is not independent. The second supervision mechanism does not address the problem of illegal access or over-collection of personal data at all, since it only excludes the probative force of the electronic evidence and does not aim to protect the right or interest of the data subjects on their personal data. It must be assessed, in the light of the GDPR's threshold concerning an "independent supervisory authority", it must be assessed that the Chinese criminal law legal system does not provide effective supervisory over the access and use of personal data by the Criminal Investigators, which also means that the data subject is granted no administrative remedy as regards the data access and use by the Criminal Investigators for criminal law purposes.

2.3 Judicial remedy for data access for the purposes of criminal law enforcement

Under the current legal framework, if a natural person considers his or her personal data unlawfully accessed and used by the Criminal Investigators during criminal investigation activities, the natural person does not have a real chance to obtain judicial remedy. The natural person could not file an administrative proceeding against the Criminal Investigators, since this presupposes the existence of an administrative act carried out by an administrative authority or its personnel under the Chinese Administrative Procedure Law, whereas the Criminal Investigators are pursuing criminal prosecutions when access the personal data.[499] The illegal access of personal

[498] Art. 56, Criminal Procedure Law.
[499] Art. 2, Administrative Procedural Law of the People's Republic of China.

data does not fall within the scope of state compensation either, according to Art. 17 of the State Compensation Law of the People's Republic of China.

3. Access by public authorities for national security purposes

3.1 Compulsory investigation for national security purposes

According to the National Security Law, the competent authorities responsible for ensuring national security are the national security authorities, public security authorities, and the relevant military authorities. A crucial duty of these competent authorities is to gather intelligence information for the purpose of national security, thus, these three departments are also the national intelligence departments.[500] According to the National Intelligence Law, the national intelligence departments may use "necessary means, methods and channels in accordance with the law" to conduct intelligence work,[501] including technical investigation measures and identity protection measures if required by the circumstances.[502] As noted in the previous section, technical investigation measures prescribed in the Criminal Procedure Law are measures with strong interference nature, such as interception of communications, record surveillance, location and activity surveillance, or premise surveillance. The implementation of these measures will inherently lead to the access of a massive amount of personal data relating to the most private sphere of the involved natural persons, without even being known by them.

Opposed to this strong interference nature, the conditions, approval and supervision of such technical investigation measures are currently not specified under the legal framework of the National Intelligence Law. The Law only states that the national intelligence departments may take technical investigation measures after going through strict approval formalities, if required by their work.[503] Since it does not specify what "strict approval formalities" the national intelligence departments have to go through, and the material condition is just "if required by work", this seems more like a general

[500] Art. 52, National Security Law; Art. 5, National Intelligence Law.
[501] Art. 10, National Intelligence Law.
[502] Art. 15, National Intelligence Law.
[503] Ibid.

authorization allowing national intelligence departments to take technical investigation measures. As demonstrated above, under the Criminal Procedure Law, in the case of a crime related to national security, the adoption of technical investigation measures should only be approved by the head of the public security authority above the city level, instead of by an independent judge.[504] If the handling national intelligence department is the public security authority itself, the approval is totally internal.

Besides, according to the National Security Law, citizens and organizations have the obligation to provide evidence of activities compromising national security to their knowledge; to facilitate or provide other assistance to national security work; as well as to provide necessary support and assistance to national security authorities, public security authorities and the relevant military authorities.[505] The national intelligence department may require any relevant department, organization or citizen to give necessary support, assistance or cooperation when conducting intelligence work in accordance with the law. This includes, of course, also the disclosure of personal data. The refusal of such support and assistance might lead to severe results for the requested organization or citizen such as being subject to disciplinary action or held criminally liable if it becomes criminally punishable.[506] Beyond this general requirement, the National Intelligence Law does not elaborate the material and procedural conditions for making such a request to an organization or citizen.

3.2 Supervision of compulsory investigations for national security purposes

The national intelligence departments must establish a strict supervision and security review system according to the National Intelligence Law, in order to supervise the compliance with the law and discipline by its personnel.[507] This supervision system is, however, inside of the national intelligence departments. It is further provided in the National Intelligence Law that any individual or organization has the right to pile a petition against the national intelligence department or any of its personnel who has acted beyond its competence, abused power or performed any other act in violation of

[504] Art. 265, Provisions on the Procedures for Handling Criminal Cases by Public Security Authorities.
[505] Art. 77, National Security Law.
[506] Art. 28, National Intelligence Law.
[507] Art. 26, National Intelligence Law.

the laws and regulations. The "relevant department" accepting the petition shall undertake investigation and handle the petition without delay and notify the petitioner of the results.[508] However, as regard to who this "relevant department" should be, the National Intelligence Law remains silent. In the absence of any further clarification, it must be concluded that no independent effective supervision of the intelligences activities has been established under the National Security Law and the National Intelligence Law.

3.3 Judicial Remedy for illegal data access for the purposes of national security

Likewise, a natural person does not have a real chance to receive judicial redress, if his or her personal data are illegally accessed by the national intelligence departments during intelligence activities. First, intelligence activities are not administrative acts, therefore, the involved natural person cannot bring up an administrative proceeding against the national intelligence departments. Further, the State Compensation Law does not apply to damages caused by intelligence activities. Only if the illegal access of personal data constitutes a crime, must the procuratorate conduct an investigation and initiate a criminal proceeding in the presence of sufficient evidence. However, this is rather unlikely due to the high standards set for a crime related to the illegal processing of personal data, as demonstrated in the previous section.

3.4 Brief summary

In general, the protection of personal data is not recognized as a fundamental right in the Chinese Constitution. In the absence of this constitutional status, the defense of data protection against access and use by public authorities is in lack of a strong legal basis of high-hierarchy.

During the criminal investigation, the Criminal Investigators may gather evidence through their own investigation measures, such as by search and seizure. under the

[508] Art. 27, National Intelligence Law.

Chinese Criminal Procedure Law, a search and/or seizure should be approved by the head of the public security authority or the procuratorate above the county level. In other words, the search or seizure of electronic data is approved internally in the Criminal Investigators system, not by an independent judge. The supervision of evidence collection also takes place within the criminal investigation authorities, thus it is in no way independent. Under the current legal framework, if a natural person considers his or her personal data unlawfully accessed and used by the Criminal Investigators during criminal investigation activities, the data subject cannot seek for judicial remedy according to the Administrative Procedure Law or the State Compensation Law, which leaves the data subject rather helpless in terms of judicial remedy.

The national security and intelligence departments may carry out investigation measures themselves or require any relevant department, organization or citizen to give necessary support, assistance or cooperation when conduct intelligence work in accordance with the law. This includes, of course, also the disclosure of personal data. While the threat to the rights of the data subject is serious, the relevant laws do not provide clear restrictions or limitations on the collection and use of personal data. In addition, the supervision of the investigation activities is established inside of the national intelligence departments. Like above, a natural person does not have a real chance to receive judicial redress in terms of the national security and intelligence measures carried out against him or her, since the measures are not administrative acts, the involved natural person cannot bring up an administrative proceeding against the national security or intelligence departments. Further, the State Compensation Law does not apply to damages caused by intelligence activities.

IV. Conclusion: Data Protection Level in China – is an Adequacy Decision About China Possible?

As it is demonstrated in chapter 3 of this dissertation, when making an adequacy assessment, the Commission needs to consider not only the substantial data protection rules in the third country in question, but also the enforcement system of that country that ensures an effective functioning of those rules in the practice, especially the

administrative and judicial redress systems. Besides, the legal framework regulating the access of public authorities to personal data in the course of criminal law enforcement or national security must also be considered. In the light of these requirements and the more detailed criterion specified in chapter 3, it must be concluded that it is rather unlikely that the EU Commission will consider the Chinese law providing a data protection level essentially equivalent to that of the EU. This judgement is based on the following four aspects as sub-conclusions of the previous analysis of this chapter, in which although the first one might favor an adequacy decision about China - at least a partial one concerning the private sector, the last three however constitute serious obstacles for China to be recognized as providing adequate protection to personal data. Subsequent to every identified deficiency improvement suggestions are made by the author.

1. The substantial data protection rules drawing close to the GDPR

From the analysis of China's substantial data protection rules in part II of this chapter, it can be observed that China has made significant progress in the protection of personal data concerning natural persons within its territory. In particular the PIPL marked a new era of China's data protection development, trending towards the direction GDPR in terms of the data processing principles, the rights of the data subject and the obligations of the data controller and processor. The Civil Code further established the protection of personal data as a personality interest that is protected under the "personality rights". Data subjects that consider their personal data illegally collected or misused now has a legal basis in civil law to bring up civil charges. Even though differences still exist, for example, the data controller is not obliged to keep a record of processing activities, it is the author's opinion that these fine differences do not significantly reduce the level of data protection in China, since the majority of the material principles and rights of the data subjects are reflected in the PIPL.

What may mark an essential difference between the current Chinese data protection law and the GDPR is the regulation of data processing by public authorities. Whereas the PIPL applies to the public authorities as data controllers, the gateway laid down in the

PIPL for data processing by public authorities needs to be specified and implemented in the relevant laws or administrative regulations. Thus, even if the PIPL applies to the public authorities as data controllers, this progress by itself is not sufficient to ensure an adequate level of protection to the personal data processed by the public authorities. Instead, in order to meet the CJEU's requirement in "Schrems II" as regards the interference of the public authority with the fundamental rights, the specific laws and administrative regulations that provide the legal basis for the data processing must also lay down the limitations and conditions on the processing, taking into account the CJEU's judgement in "Schrems I" and "Schrems II".

2. The right of the data subject to administrative remedy and judicial remedy

According to Art. 65 PIPL, the data subject has a right to lodge a complaint with the relevant competent supervisory authority. In this sense, the problem of administrative remedy lies rather in the uncertainty of finding the right competent supervisory authority among the various departmental ministries and the lack of the independent status of such supervisory authorities.

The PIPL does not generally provide data subjects a right to judicial remedy, it only states in Art. 50 that if the data controller refuses the data subject's request to exercise data subjects' right, the data subject may bring a suit to the court. In other cases, for example if the data controller violates the data processing principles or other obligations of the data controller, and the data subject wishes to seek judicial remedy, he or she has to turn to the more general laws, namely the Civil Code and the Administrative Procedure Law. The Administrative Procedure Law generally allows a natural person to challenge the omission or decision of an administrative authority relating to the protection or violation of a natural person's personality rights in the court. Besides, a data subject who considers his or her personality rights and interests on the personal data have been infringed also has the right to directly bring a civil proceeding against a data controller or processor who is a private body based on the Civil Code, and an administrative proceeding against a data controller or processor who is an

administrative authority based on the Administrative Procedure Law. However, as observed above, the general rules under the Administrative Procedure Law and the State Compensation Law do not apply to the data access by the law enforcement authorities and intelligence authorities, which leaves such data access activities by the law enforcement authorities and intelligence authorities unregulated. Unlike the GDPR, the PIPL failed to introduce a provision expressly granting the data subjects a right to bring an action against any data controller or processor, including the law enforcement authorities and intelligence authorities, and against the decision of a supervisory authority before the court.

3. The lack of effective implementation and enforcement of the substantial rules

A much bigger problem of the Chinese data protection law in the light of the European standards lies in the lack of an effective implementation, supervision and enforcement of the material rules. None of the laws analyzed above establishes an independent data protection supervisory authority. The supervision competences are largely in the hands of the various departmental ministries, which are neither delimited from each other nor reasonably coordinated. This approach, that the ministry competent for the overall development of the respective department is at the meantime the supervisory authority for data protection issues within that department, inevitably leads to a conflict of interests. This generally results in the need of economic development or social governance overwhelming the rights and interests of the data subject. It is a common phenomenon in China that a specific data-based branch is able to develop very fast without serious data protection supervision at first, until a large number of scandals of misusing personal data are revealed, the competent departmental ministry will then start an enforcement campaign. In this sense, one can conclude that the supervision of the compliance with the substantial data protection rules occurs only on an irregular, unsystematic basis. The current stand is that the State Cyberspace Administration is responsible for the coordination, the supervision and the administration of the data protection implementation under the PIPL. However, the State Cyberspace Administration is an administrative office in charge of the implementation of

cyberspace related policies and laws under the State Council, which is the highest executive organ of the P.R.C.[509] Currently, there is no special guarantees regarding the personnel selection and financial budgets of the State Cyberspace Administration. Actually, the directors of the State Cyberspace Administration hold concurrent posts in other departments at the same time.[510] As the CJEU denied the independence status of the "Ombudsperson" in "Schrems II" due to its executive subordination,[511] it is foreseeable that the State Cyberspace Administration with its current setting will not be considered independent from the executive. In that sense, if the State Cyberspace Administration is to act as an independent data protection supervisory authority, it must be able to remain free from any direct or indirect external influence, and be granted with separate, sufficient human, technical and financial resources by law, in order to perform its functions effectively and independently.

4. The wide access of personal data by public authorities for the purpose of criminal law enforcement and national security

After an investigation into the relevant rules concerning the public authorities' access to personal data for the purpose of criminal law enforcement and national security, part III of this chapter comes to the conclusion that the Criminal Investigators and the national security and intelligence departments have general access to the personal data of natural persons. In particular the access personal data for purposes of national security is generally authorized without being limited to a specific identified threat to national security. Furthermore, there is no independent supervision for the data processing activities of the public authorities in this specific field. Generally, the evidence collection and investigation activities of these public authorities are rather supervised within their own systems, for example by their superior or by the procuratorate, a court warrant as appeared in many countries is not needed under the Chinese law. The data subject also lacks the access to judicial remedy, since the Civil Code and the Administrative Procedure Law do not apply to the criminal law

[509] State Council of the P.R.C., Announcement of the State Council About the Organizational Structure, 22.03.2018.
[510] Announcement of the General Office of the State Council Regarding the Establishment of the State Cyberspace Administration.
[511] CJEU, C-311/18, 16.07.2020, para.195.

enforcement activities and matters concerning national security, nor does the illegal processing of personal data fall within the scope of the State Compensation Law. This unsatisfying status quo cannot be improved by merely introducing one single mechanism like the “Ombudsperson” in the EU-US “Privacy Shield”, whose effectiveness has already been rejected by the CJEU. Instead, a substantial improvement could only be achieved by a systematic amendment of the Criminal Procedure Law and the National Intelligence Law, by laying down precisely the legal basis, the scope, the application conditions and the limitations of the data access by criminal law investigators and intelligence authorities. Meanwhile, the problem regarding the effective supervisory and implementation could have been solved by establishing an overall independent data protection supervisory in the comprehensive PIPL, and the judicial remedy within the framework of introducing an explicit right of the data subjects to a judicial remedy against all data controllers or processors, as already suggested in the above sections, however, the PIPL has missed the chance.

Chapter 5 Data Transfers Based on Appropriate Safeguards and Derogations

I. Data Transfers from an EU Based Data Controller to a Chinese Controller or Processor

If personal data are transferred by a data controller established in the EU to a data controller or processor located in China, for example, when Amazon Germany transfers personal data of a German buyer to a Chinese seller, Art. 46 GDPR contains an array of measures to provide appropriate safeguards for the data transfer. Nevertheless, not all the measures contained in Art. 46 GDPR can be relied upon to transfer data in a specific circumstance in the cross-border E-Commerce context. In the following, typical scenarios of data flows from an EU based data controller to a Chinese controller or processor will be analyzed, based on which it will be analyzed which kind of measures can be taken to provide appropriate safeguards for data transfers from the EU to China.

1. EU established E-Commerce platforms transferring personal data to Chinese sellers

Platforms such as Amazon and Wish have a vast number of Chinese sellers. When orders are placed by EU buyers, in general, platforms have to send the buyer's basic data to the seller and logistic partners to fulfill the order. Thus, personal data concerning the EU data subject are transferred across the EU border to China.

In such cases, when trying to find an appropriate legal basis for the data transfer, it is important for the platforms to notice the layered approach that was advocated by the WP 29 and subsequently endorsed by the EDPB. Namely, the data controller or processor should consider first whether the involved third country was recognized by the EU Commission as providing an adequate level of protection. If such adequacy decision does not exist, they should try to take appropriate safeguards. Only if appropriate safeguards are impossible or puts undue burden on the data controller or

processor, the data controller or processor may consider to rely on the derogations contained in Art. 49 GDPR to enable the data transfer.[512] Since there is no adequacy decision on China issued by the EU Commission, the data controller has to endeavor to take appropriate measures first, in order to safeguard the personal data that are to be transferred to China.

1.1 Standard Contractual Clauses

Under the appropriate safeguards laid down in Art. 46, SCCs seem to be the most practical option, since the discussed transfer here does not take place within a group of enterprises, so that the binding corporate rules could not apply, nor can the data controller force the numerous Chinese sellers to adherence to an approved code of conduct or an approved certification mechanism. The SCCs are probably also the easiest option for the EU data controller to provide appropriate safeguards to the transfer, given that the European Commission has issued SCCs for both scenarios: data transfers from an EU controller to a non-EU controller and or a non-EU processor.

A barrier of using the SCCs for transferring personal data to the Chinese sellers is the large number of Chinese sellers on dominant platforms such as Amazon. Platforms might assert having difficulties to establish SCCs with every single seller given the huge number it involves. However, that argument could not really stand since platforms will enter into contracts with the Chinese sellers regardless when the latter register on the platform of the former. Platforms are hence able to integrate the data protection SCCs into those contracts or make a new data protection contract with the Chinese sellers without causing them excessive burden. This is particularly justified, given the rich resources cross-border E-Commerce platforms usually have, and the rather stable business relationship between the platforms and the sellers.

A genuine obstacle of transferring the personal data to China based on the SCCs in this scenario is, however, that the Chinese laws grant the intelligence authorities and

[512] EDPB, Guidelines 2/2018 on derogations of Art. 49 under Regulation 2016/79, adopted on 25 May 2018, p.3; Art. 29 Working Party, Working Document on a Common Interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995, adopted on 25 November 2005, p.9.

criminal law enforcement authorities access to personal data, without defining the scope and conditions of such data access clearly and precisely. In addition, data subjects are not granted with actionable rights and effective legal remedy regarding such data access by public authorities. This was analyzed in chapter 4. In the light of the "Schrems II" judgment, this kind of access cannot be considered as limited to what is necessary and proportionate in a democratic society. Thus, the question arises whether supplementary measures are necessary.

1.1.1 Arguments against the adoption of supplementary measures

Based on the risk-approach, one might still argue that personal data generated during the cross-border e-commerce, in contrast to telecommunication data or social network data, has little significance for intelligence or criminal law enforcement actions, thus it is rather unlikely that the intelligence authorities and criminal law enforcement authorities will request access to these data. This argument is further strengthened by the negative result of a search on internet for news and reported precedents regarding personal data access requests made by public authorities against cross-border e-commerce operators. If one follows the position of the Commission in the New SCCs, namely the assessment of the laws in the third country should take account of the specific circumstances of the transferred personal data and "relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests"[513], one could come to the conclusion that the laws concerning the intelligence and criminal law enforcement activities does not really impinge on the effectiveness of the SCCs, since, practically, there is no risk of the personal data transferred being subject to those laws. Following this assessment, the SCCs could be relied on to transfer personal data to China in the scenario discussed here without adopting supplementary measures.

[513] Footnote 12 of the New SCCs.

1.1.2 Arguments for the adoption of supplementary measures

However, there are also counter arguments in this regard. First, the E-Commerce Law of the P.R.C., which directly applies to the operators of the cross-border e-commerce, it is stated that "*where the relevant authorities require, according to any law or administrative regulation, an e-commerce business to provide relevant e-commerce data and information, the e-commerce business shall do so.*"[514] This provision indicates that there is a possibility that public authorities might actually ask a e-commerce business operator to provide e-commerce data, which might also include personal data. It is also not to exclude that if a cross-border e-commerce operator is subject to law enforcement measures, for example due to tax evasion or violation against import and export regulations, personal data of its overseas customers would be disclosed to the law enforcement authorities. According to the EDPB's position in the Recommendation on Supplementary Measures, the effectiveness of the SCCs is impinged, since the assessment "must be based first and foremost on legislation publicly available",[515] and "the absence of prior instances of requests received by the importer can never be considered, by itself, as a decisive factor on the effectiveness of the Article 46 GDPR transfer tool that allows the transfer to proceed without supplementary measures"[516]. Due to the existence of the above-mentioned legislation, the data importer in China cannot prevent the personal data transferred from data access by public authorities that is not necessary and proportionate, and the data subjects will have no actionable rights or legal remedy against such access. If one follows this position, the next step is, as recommended by the EDPB in its Recommendations on Supplementary Measures, for the data exporter in the EU in collaboration with the data importer in China to take supplementary measures to render such data access by public authorities impossible. In this regard, the EDPB has noted that contractual and organizational measures alone are generally not be able to overcome data access by public authorities,[517] since these contractual or organization-internal measures due to their very nature are not binding to public authorities. In such cases, technical measures might be the only choice. The EDPB has listed in annex 2 of the Recommendations on

[514] Art. 25, E-Commerce Law of the P.R.C., adopted on 31.08.2018.
[515] EDPB, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, Version 2.0, adopted on 18 June 2021, para. 43.
[516] Ibid, para. 47.
[517] Ibid, para. 53.

Supplementary Measures 5 case groups, in which even if the data access by public authorities in the third country goes beyond what is necessary and proportionate, these technical measures still apply and can ensure an essentially equivalent level of protection. In these 5 case groups, 4 of them require that the personal data are so strongly encrypted, pseudonymized or split up, that the personal data cannot be attributed to a specific data subject by the data importer or the public authorities requesting access, and the last one applies to the case in which the recipient is subject to protection laws of the third country that exempts the data importer from potentially infringing access.[518] In the scenario discussed here, the EU established e-commerce platforms need to send personal data of the customers to the Chinese seller in order to fulfill the purchase order or service requests. To that end, access to data in the clear will most probably be needed by the Chinese seller, encrypted or pseudonymized data would be no help to achieve that purpose. The above mentioned 5 use cases of technical measures do not fit. If no effective supplementary measures can be found, the data exporter would have to suspend the data transfer.

1.1.3 Observation and suggestion

As discussed previously in chapter 3 section 2.5.4 of this dissertation, whether subjective factors, such as the likelihood of the data access by public authorities, should be relied upon to the assess the legal situation of the third country, can make a substantial difference. If we follow the position that such factors should not be relied upon, and reach a decision merely based on the pure theoretical possibility of data access by public authorities due to the existence of a vague drafted legislation, the result would be technical supplementary measures must be in place. The hard reality then reminds us that there are no effective technical supplementary measures available according to the opinion of the EDPB. A responsible data exporter then needs to suspend the data transfer, or if applicable, transfer the personal data based on derogations that provide no extra protection to the personal data at all. None of these two results seem to be ideal. On the one side, if data transfers as common as this must

[518] EDPB, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, Version 2.0, adopted on 18 June 2021, para. 84-92.

be suspended due to the unavailability of a legal basis, the cross-border commercial activities might just come to an end. However, it is also in the interest of the data subjects to have their data transferred based on SCCs that at least provide some protection than on derogations, which leave them nothing.

The considerations above make it appear reasonable to the author that the assessment of the laws of the third country should be based on a risk-based approach as indicated in the Commission's New SCCs. This means, first, the assessment should take account of the nature of the personal data to be transferred. In the course of cross-border e-commerce platforms transferring personal data of the customers to Chinese sellers, the involved data are for example names, addresses, contact info, and sometimes also payment information. Payment information can be sensitive and should only be provided to the Chinese seller when strictly necessary. The other personal data do not belong to special categories of personal data and are not sensitive as, for example, health data, telecommunication data, political opinions etc. The threshold for safeguarding these personal data should not be set as high as personal data that belong to special categories, given that the purpose of the transfer is duly justified. Bearing this in mind, the assessment of the legal system in the third country should consider the likelihood of the data access by public authorities, not the mere existence of a law that allows generalized access. By assessing the likelihood of the data access by public authorities, the parties can give due consideration to factors such as whether the data importer or its alike has received access requests by public authorities, directly or indirectly, reported precedents etc. If there has been precedents or news indicating that a real possibility of data access by public authorities exist, the law of the involved third country should be considered as impinging on the effectiveness of the appropriate safeguard, the data transfer must be suspended in the absence of effective supplementary measures. To avoid random or inconsistent assessments among different data exporters, the Commission or the EDPB can issue branch-specific guidance providing information regarding access request precedents. On the contrary, if the personal data to be transferred are special categories of personal data or other sensitive data, the mere existence of a law that allows generalized access which does not grant the data subjects actionable rights and legal remedies should be enough to lead to a negative assessment result, and the data transfer must be suspended in the absence of

effective supplementary measures.

If one follows this risk-based approach, the result would be, SCCs provide appropriate safeguard to the data transfer from the EU established cross-border e-commerce platforms to Chinese sellers, without the adoption of supplementary measures being necessary.

1.2 Derogations

It could also be an option to carry out the above-discussed data transfer based on some of the derogations provided in Art. 49. However, the derogations as legal basis for the transfer data across the EU border are considered exemptions from the general principle and must be interpreted restrictively, in order to provide an appropriate protection to the data subjects' fundamental right.[519]

1.2.1 Data transfer is necessary for the performance of a contract

The first legal basis to consider is Art. 49 section 1 (b), namely the data transfer is necessary for the performance of a contract between the data subject and the controller. The data transfer from the platform to a Chinese seller is necessary for the fulfillment of the service contract between the buyer and the platform, as well as for the sales contract between the seller and the buyer. However, it is the opinion of the EDPB that this exemption should be limited to occasional data transfers,[520] based on Recital 111 GDPR, which explicitly states that the transfer in relation to a contract should be "occasional"[521]. It remains questionable whether the data transfer between the E-Commerce platforms and the sellers located in a third country could be considered occasional. According to the EDPB, occasional data transfers refer to transfers that "may happen more than once, but not regularly, and would occur outside the regular course of actions, for example, under random, unknown circumstances and within

[519] SCHRÖDER, Christian, Art. 49, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H.BECK, 2nd Edition 2020, p.2.
[520] EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/79, adopted on 25 May 2018, p.3.
[521] Recital 111, GDPR.

arbitrary time intervals"[522]. It further notes that if there is a stable relationship between the data exporter and the data importer, and the data transfer happens within that relationship, the data transfer could most probably be seen as systematic and repeated.[523] Against this background, since it can be argued that platforms have a stable relationship with the Chinese sellers, it is possible that the data transfers between them are deemed systematic, thus not occasional by the data protection authority. Due to this risk, relying on Art. 49 section 1 (b) to transfer data to Chinese sellers is not a satisfying option.

1.2.2 Explicit consent of the data subject

Another derogation that may come into sight is the explicit consent of the data subject pursuant to Art. 49 section 1 (a). Unlike the derogation of data transfer necessary for the performance of a contract, the consent derogation is not limited to data transfers that are occasional.[524] It means, personal data can be transferred to a third country based on the explicit consent of the data subject in repetitive cases. Nevertheless, since relying on the explicit consent of the data subject to carry out data transfer is still an exception from the general conditions for data transfer, the data controller should not use consent as a first option, if appropriate safeguards are practical and possible in individual cases.

In addition, there are certain conditions that consent needs to meet in order to be able to justify the data transfer. First, consent of the data subject needs to be explicit, meaning the data subject has to give an express statement of consent.[525] Therefore, an implied, affirmative action of the data subject is not an explicit consent. Second, consent given by the data subject must be specific for the intended data transfer. This means, first, consent must be specific, which excludes all-encompassing consent. Second, the data controller has to inform the data subject about the cross-border nature of the transfer, and the fact that the third country to which the personal data are intended to be transferred does not provide an adequate level of protection and no appropriate

[522] EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/79, adopted on 25 May 2018, p.4.
[523] Ibid.
[524] Ibid, p.5.
[525] EDPB, Guidelines 05/2020 on Consent under Regulation 2016/679, adopted on 4 May 2020, p.18.

safeguards are in place.[526] Only when the data subject has fully perceived the risks the intended data transfer might bring along, the consent is given specifically and truly informed.

2. EU established E-Commerce platforms or sellers transferring personal data to Chinese service providers

As service and business solution becomes more and more global structured, there are circumstances where EU established E-Commerce operators engage Chinese solution providers such as cloud providers or logistic partners to implement their business operations. In the course of such cooperation framework, personal data might be transferred from the EU to China.

Likewise, since there is a stable relationship between the E-Commerce operators and the service providers in such cases, the proper safeguard for data transfer would be adopting SCCs, as analyzed above. The derogations laid down in Art. 49 should not be relied upon as legal bases to conduct the cross-border data transfer, due to the priority of providing appropriate safeguards when it is possible, since the derogations themselves do not provide any extra protection to the data transferred.

II. Data Transfers from the EU to non-EU Data Controllers Subject to the GDPR per Art. 3

Due to the online nature of E-Commerce, operators or participants do not necessarily have to be established on the target market to conduct business there. Therefore, some Chinese sellers or service providers only have establishments in China but making use of the boundless nature of the internet to attract potential customers all over the world, including that from Europe. These include, for example, Chinese cloud services providers, consulting companies, travel agencies, electronic products producers, etc. Other Chinese E-Commerce operators take advantage of some worldwide famous free

[526] EDPB, Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/79, adopted on 25 May 2018, p.7-8.

harbors, such as Hong Kong or Singapore, and establish offices to expand their business to the rest of the world. A classic example here is the international version of the second-biggest Chinese E-Commerce platform Jindong, whose international station Joybuy is based on Hong Kong and sell products from there to Europe, America and other Asia countries. In addition, there are data analysis companies that provide tracking or monitoring services for these E-Commerce operators. The common feature of these E-Commerce participants discussed here is that they are located outside of the EU, but collect personal data on the EU market and have a need to transfer such data outside of the EU.

In terms of personal data processing operations carried out by data controllers that are not established within the EU, it would be reasonable to make a distinction between two circumstances.

Under circumstance 1, the data controller located outside of the EU engages a data processor in the EU to help it processing personal data of the EU data subjects. In this circumstance, personal data of the EU data subjects are stored and processed by the EU data processor first, only later will they be transferred from the EU processor to the data controller located in the third country. Some Chinese companies make such kind of arrangements such as Aliexpress, who states in its privacy policy that the personal data concerning to the EU data subjects will be first stored in Germany.[527]

Under circumstance 2, personal data of the EU data subjects are transferred to the data controller established in China directly when they are collected. This is usually the case when small to medium sized Chinese companies provide online products such as games, travel services, beauty products to the EU market. In this circumstance, personal data of the user of these web shops or Apps are directly transferred to the server that holds the web shops or Apps. The same could also happen with bigger E-Commerce platforms, for instance Joybuy did not mention in its privacy policy that personal data of the EU data subjects are stored within the EU, the author assumed from the general text of the privacy policy that the data are centered in somewhere else possibly where the data

[527] AliExpress.com Privacy Policy, adopted on 26.12.2019, section J "Visitors from the European Union", available at https://service.aliexpress.com/page/knowledge?pageId=37&category=1000022028&knowledge=1060015216&language=en, last visited on 06.05.2021.

controller is located, namely Hong Kong or mainland China, where the headquarter of the company group locates.[528] In such case, the collection and transfer of personal data are *de facto* not separable. As noted in chapter 3 of this dissertation, under this circumstance, there is no data controller or processor within the EU. Whereas the transferor that exports the personal data from the EU to the third country may be considered the data subject itself, this interpretation faces several major challenges. First, Art. 46 GDPR seems to indicate that the transferor should be a data controller or processor. Besides, since the data subject is not the target group of the compliance obligations under the GDPR, making the data subject the transferor does not lead to any extra safeguards for the personal data transferred to the third country. Nonetheless, the data controller in the third country may be considered as the transferor too, since he or she is the one that collects the personal data and decides where they are to be sent. It does not go against the system of Art. 46. Theoretically, in the case of using codes of conduct or data protection certification mechanism as appropriate safeguards, it is only required that the data controller or processor in the third country applies the appropriate safeguards. Thus, even if there is no data controller or processor in the EU, the data controller or processor located outside of the EU may still transfer data to a third country based on codes of conduct or certification mechanism.

Following this logic, the more important issue is, whether the appropriate safeguards laid down in Art. 46 to justify data transfers from the EU to a third country under the GDPR are practically applicable to the above two circumstances. This will be elaborated in a more detailed way below.

1. Data transfer from EU data processors to Chinese controllers that are subject to the GDPR per Art. 3

Data processors now explicitly belong to the target group of the data transfer rules under Chapter V GDPR, which means, if an EU data processor transfers personal data to a third country, it should make sure that the conditions for data transfer from the EU to a

[528] Joybuy Privacy Policy, adopted on 24 May 2018, available at https://help.joybuy.com/help/question-535.html, last visited on 06.06.2021.

third country laid down in Chapter V GDPR are met. This should also apply, according to the wording of Chapter V GDPR and the reasons demonstrated in chapter 2 and 3 of this dissertation, when the EU data processor transfers personal data to the data controller located outside of the EU that is subject to the GDPR as per Art. 3. However, in contrast to this enhanced obligation of the data processor within the framework of data transfer to a third country under the GDPR, the legal bases that a data processor may use to justify a set of data transfer to a third country is not broadened. As a result, the data processor is imposed with the obligation to comply with the conditions laid down for data transfer from the EU to a third country but lacks the means to do so. This will be illustrated by the following examination as to whether each legal basis can apply to the discussed data transfer:

1.1 Binding corporate rules

Binding corporate rules may only come into consideration, if the EU data processor and the non-EU data controller belong to the same group of undertaking or group of enterprises engaged in a joint economic activity, and the group has drafted a set of binding corporate rules which was approved by the competent supervisory authority according to Art. 47 GDPR. While this is not impossible, the application scope of this approach is restricted under the framework of China-EU cross-border E-Commerce. First, as demonstrated above, many E-Commerce operators are small or medium sized, so that there is no group of enterprises. Second, even if the E-Commerce operator is part of a group of enterprises, an approvable set of binding corporate rules presumes strict conditions, which makes the application of it in business practically difficult.

1.2 Standard contractual clauses

One might also consider using SCCs as a legal basis to justify the data transfers from an EU data processor to a data controller established in a third country. However, whoever attempts to do so will quickly run into difficulties, since the Old SCCs issued by the Commission under the Data Protection Directive only refer to the “controller to

controller" scenario and "controller to processor" scenario. In this regard, the New SCCs, which covers also the module from processor to controller, does not bring much help.[529] Whereas the Draft New SCCs did not exclude the application of the module "processor to controller" to data transfer from a EU processor to a controller that is established in a third country but subject to the GDPR per Art. 3 (2),[530] the officially adopted New SCCs explicitly left out the scenario discussed here by stating that "the SCCs may be used for such transfers only to the extent that the processing by the importer does not fall within the scope of Regulation (EU) 2016/679".[531] Although, at the same time, it is provided in the same paragraph of the New SCCs that a controller or processor may use these SCCs to provide appropriate safeguards for the transfer of personal data to a processor or controller established in a third country, **without the prejudice to the interpretation of the notion of international transfer in Regulation (EU) 2016/679 (emphasis added by the author).**[532] This seems to indicate that the Commission does not intend to exclude the possibility that data flows from the EU to a data importer established in a third country but subject to the GPDR per Art. 3 (2) may still fall into the scope of an international data transfer within the meaning of Chapter V GDPR. Only it should not use the SCCs as a legal basis. If one follows this interpretation, it is indeed very confusing what could be the proper legal basis for data flows from an EU processor to a controller that is established in a third country but subject to the GDPR per Art. 3 (2). Or, one must indeed assume that data flows from a EU processor to a controller that is established in a third country but subject to the GDPR per Art. 3 (2) should not be considered an international data transfer within the meaning of Chapter V GDPR at all, thus no extra legal basis is needed? In this sense, again, the concept of data transfer within the meaning of Chapter V GDPR is in urgent need of further explanation. In the author's opinion, the position in the Draft New SCCs is more recommendable, namely, module four "processor to controller" also applies to transfers of personal data to a data importer that is subject to the GDPR. The reason is

[529] New SCCs, module four.
[530] See Draft implementing decision on SCCs for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, recital (7).
[531] Commission Implementing Decision (EU) 2021/914 of June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, recital (7), sentence two.
[532] Commission Implementing Decision (EU) 2021/914 of June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, recital (7), sentence one.

that, as demonstrated in chapter 2 and 3 of this dissertation, the mere fact that the data importer is subject to the GDPR per Art. 3 (2) does not ensure an adequate protection of the personal data transferred to a third country.

In chapter 3 of this dissertation, it is illustrated why the data transfer rules under Chapter V GDPR should still apply, even if the data importer in the third country is subject to the GDPR per Art. 3 (2). One of the reasons is precisely the data access by public authorities in the third country. While the effect of the direct application of the GDPR in a third country per Art. 3 (2) might be impaired by the local laws of the third country, especially those allowing data access by public authorities, in the case of data transfer to a third country, the local laws of the third country always play a role and should always be taken into consideration, no matter in the course of an adequacy decision by the Commission or when applying the appropriate safeguards. Even though the assessment of the local laws of the third country and the adoption of supplementary measures to ensure an adequate level of protection in the third country remains challenging in the after "Schrems II" era, the Commission's New SCCs and the EDPB's Recommendation on Supplementary Measures has responded to this issue, by which the first step towards a workable solution is already taken.

In addition, the application of the data transfer rules under Chapter V GDPR to data transfers to data importers that are already subject to the GDPR per Art. 3 (2) may also be a useful way to solve the enforcement problem of Art. 3 (2). With regard to the SCCs applicable to data transfers from a EU processor to a non-EU controller, in the case of both the data exporter and importer being responsible for the damages caused by a breach of the clauses, the joint and several liabilities of the parties against the data subjects makes it possible for the data subject to hold the data exporter in the EU liable. The data exporter in the EU is then entitled to receive indemnification from the data importer for the latter's share in the liability. Since there is a contractual relationship between the parties, the enforcement of this indemnification obligation of the data importer should not be too difficult for the data exporter, who itself is usually an enterprise with relatively more resources than the individual data subject.

Against this background, in the author's opinion, there is no reason why the module four "data transfer from processor to controller" should not apply to transfers to data

importers that are already subject to the GDPR per Art. 3 (2). The Commission or the EDPB might need to shed more light on this matter in the future.

1.3 Codes of conduct and data protection certification as appropriate safeguards for data transfers from EU processors to controllers in a third country

Codes of conduct and certification mechanism are new forms of appropriate safeguards introduced by the GDPR. The contents and application conditions of these two forms are already illustrated in chapter 3 of this dissertation.

1.3.1 Applicability of codes of conduct and certification

These two mechanisms are analyzed here together, because they have several features in common: first, they are both co-regulation tools[533] managed by an independent third party, mostly private bodies, except for the case that the certification body is the competent supervisory authority. Second, both are direct applicable to the data importer, namely data controllers or processors located in a third country.[534] Art. 46 section 2 (e) and (f) only require the data importer in the third country to make binding and enforceable commitments to apply the appropriate safeguards. In this regard, no obligation is imposed on the data exporter. In terms of the status of the data importer in the third country, it should be understood as, data controllers or processors established in a third country, whether subject to the GDPR per Art. 3 or not, could all benefit from the codes of conduct and certification as justification for data transfers to third countries. This interpretation is reasonable, because according to Art. 40 section 3 and Art. 42 section 2, codes of conduct and data protection certification mechanisms may be adhered to, in addition by controllers or processors subject to the GDPR, also by controllers or processors that are not subject to the GDPR pursuant to Art. 3, for the

[533] VOIGT, Paul, Art. 49, in: SPINDLER, Gerald; SCHUSTE, Fabian, Electronic Media Law (Recht der elektronischen Medien), C.H. Beck, 4th Edition 2019, p. 18.

[534] Some scholars consider that Art. 40 section 3 presents a contradiction with Art. 46 section 1, see KUNER, Christopher, Art. 46, in: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher. The EU Data Protection Regulation (GDPR): A Commentary. Oxford University Press, Oxford, 1st Edition 2020, p. 807: "Art. 46 section 1 refers to appropriate safeguards that are provided by the data controller or data processor transferring personal data from the EU, not by the parties receiving the data".

purpose of providing appropriate safeguards to personal data transferred to third countries.

Thus, codes of conduct and certification mechanisms can also be used for the scenario data transfers from processor to controller, as long as the additional conditions required for the codes of conduct and certification mechanisms as appropriates safeguards are met.

1.3.2 Enforcement of Codes of conduct and certification

Besides, the application of codes of conduct and certification mechanisms also have advantages with regard to the supervision of GDPR-compliance of the data controller in the third country. As demonstrated in chapter 2, the supervisory authorities have very limited resources to supervise the compliance with the GDPR by the data controller in the third country. This problem can be better solved with codes of conduct and certification mechanisms. Under any code of conduct, there must be a monitor body that monitors the compliance with the code of conduct, which is independent and has expertise in data protection.[535] The monitoring body also has the competence to take appropriate actions in cases of infringement of the codes of conduct, including contractual penalties.[536] For codes of conduct that aim at providing appropriate safeguards for data transfers to third countries, the monitor mechanism, which is an indispensable part of a code of conduct, must be in the position to monitor the compliance of the data controller or processor in the third country that adheres to it, and enforce sanctions directly in the third country where the data controller or processor locates. This is an inherent requirement for codes of conduct that are drafted for the purpose of providing appropriate safeguards for data transfers to third countries. It is exactly this feature that makes codes of conduct a better enforcement tool than "hard enforcement" by data protection supervisory authorities or judgements of EU courts.

[535] Art. 41 section 2, GDPR.
[536] ROSSNAGEL, Alexander, Art. 40, in: SIMITS, S.; HORNUNG, G.; SPIECKER gen. DÖHMANN, I, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, p. 54; BERGT, Matthias; PESCH, Paulina Jo, Art. 40, in: KÜHLING, Jürgen; BUCHNER, Benedikt. GDPR - Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 22.

The same also applies to the certification mechanisms. The certification body has to monitor the compliance of the controller or processor in the third country with the GDPR according to the certification criteria.[537] If the processing activities of the controller or processor in the third country no longer meet the certification criteria, the certification must be withdrawn.[538] In conclusion, the monitoring body and certification body has more resources and a more recognizable contractual legal basis to conduct supervision and enforcement against the data controller established in the third country.

In addition, the data controller in the third country must make binding and enforceable commitments to allow the data subjects to exercise their rights. The most feasible way to achieve this is per contractual means.[539] For the scenario data transfers from a EU processor to a non-EU controller established in a third country, these commitments could be made through an third-party beneficial agreement between the owner of the code/the certification body and the controller in the third country, or between the processor and the controller in the third country, or that the data controller in the third country makes a unilateral self-binding declaration against the data subjects, that it accepts the exercise of the data subjects' rights. Making commitments in the form of a contract or unilateral promise is a legal act based on the data controller's own will, which is allowed in a lot of jurisdictions, for example in Art. 134 of the Chinese Civil Code,[540] thus, the data controller cannot revoke jurisdiction objection to deny enforcement, if the data subject wishes to exercise their rights through judicial proceedings.

1.3.3 Problems in the application of the codes of conduct and certification mechanisms

Under the Data Protection Directive, the practical significance of codes of conduct and

[537] European Commission, Directorate-General for Justice and Consumers, BODEA, G., STUURMAN, K., BREWCZYŃSKA, M. et al., Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679 – Final report, Publications Office, 2019, p. 175.
[538] Art. 43 section 3, GDPR.
[539] SCHANTZ, Peter, Art. 46, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, p. 8.
[540] Art. 134 of the Chinese Civil Code provides that legal transactions could be established both by bilateral or multilateral consensus and unilateral intent.

certifications was almost negligible since there were very few of them approved. In Germany, there were only two codes of conduct approved by the respective competent supervisory authority under the Data Protection Directive.[541] It must be noted that under the era of Data Protection Directive, codes of conduct and certifications were not recognized as appropriate safeguards that provide legal basis for transfer of personal data to third countries.

Under the GDPR, codes of conduct and certifications now have the potential to help small and middle-sized controllers or processors in third countries to demonstrate appropriate protection to personal data originated from the EU. However, notwithstanding all these promising benefices, after more than 2 years of effectiveness of the GDPR, there is still no approved code of conduct that is declared to have general validity within the EU by the EU Commission,[542] which is largely considered the prerequisite for codes of conduct to serve as legal basis for data transfers to third countries. Against this backdrop, codes of conduct are appealing but practically unavailable for small and middle-sized controllers and processors who have a need for data transfers from the EU to a third country. Likewise, there are no certification criteria that have been approved by the competent authority or EDPB yet for data transfers from the EU into third countries.[543]

1.3.3.1 General challenges faced by co-regulation

The reasons for this lack of practical significance are multi-fold. As an art of co-regulation, codes of conduct and certification mechanisms are confronted with problems that are generally faced by co-regulation. The challenges faced by co-regulation were summarized by well-known scholars as the ones concerning standard-setting and standard-enforcement, as well as those concerning the general framework

[541] BERGT, Matthias, The Importance of Codes of Conduct and Certification under the General Data Protection Regulation (Die Bedeutung von Verhaltensregeln und Zertifizierungen nach der Datenschutz-Grundverordnung), Smart World-Smart Law, 2016, pp. 484.
[542] ARMINGAUD, Claude-Etienne, EU Data Protection: in a Post-Privacy Shield, Sectoral Code of Conduct Could Lead the Way to Safeguard Data Transfers Outside the EU/EEA, 17.07.2020, available at https://www.klgates.com/eu-data-protection-in-a-post-privacy-shield-sectorial-code-of-conduct-could-lead-the-way-to-safeguard-data-transfers-outside-the-eueea-07-17-2020, last visited on 04.12.2020.
[543] European Commission, Directorate-General for Justice and Consumers, BODEA, G., STUURMAN, K., BREWCZYŃSKA, M. et al., Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679 – Final report, Publications Office, 2019, p. 194.

surrounding the co-regulation.[544] More specifically, in terms of the standard-setting, the standards set in the co-regulation must fulfill certain minimum requirements, such as they must be consistent with the statutory provisions, guarantee the participation of the essential stakeholders and transparent procedure etc.[545] With regard to the enforcement of the standard, it must be guaranteed that the participants make binding commitment to implement the standard. There must also be effective mechanisms to monitor the implementation of the standard as well as effective complaint mechanism and sanctions to accelerate the enforcement against violations.[546] Another crucial factor affecting the effectiveness of the co-regulation is the general framework surrounding the co-regulation. In this regard, the scholars have argued that state institutions should play an active role in the co-regulation by providing both positive and negative incentives to accelerate the application of the co-regulation.[547] It is also demonstrated that in some EU Member States, such as in Germany, the state institutions are generally skeptical about the effective enforcement in co-regulation.[548]

1.3.3.2 Specific problems concerning the practical relevance of the codes of conduct and certification mechanisms under the GDPR

Regarding the codes of conduct and certification mechanisms under the GDPR specifically, it is the author's opinion that the aforementioned challenges concerning the standard-setting and standard-implementation are largely addressed and responded to in the GDPR. As demonstrated in the previous sections, the requirements imposed on the codes of conduct and certification mechanisms as legal bases for data transfers from the EU to a third country are highly stringent. The codes of conduct or certification criteria must be approved by the data protection supervisory authority. The decisive factors for the approval are compliance with the statutory rules and the level of protection provided to the data subject. Thus, the standard-setting is under direct supervision of the supervisory authority. In terms of the enforcement of the standards,

[544] SPINDLER, Gerald; THORUN, Christian, The Role of Co-Regulation in the Information Society-Recommendation for Action on Digital Governance (Die Rolle der Ko-Regulierung in der Informationsgesellschaft-Handlungsempfehlung für eine digitale Ordnungspolitik), MMR-Beil, 2016, No. 6, pp. 1.
[545] Ibid, p. 3.
[546] Ibid.
[547] Ibid.
[548] Ibid, p. 4.

Art. 41 GDPR requires the monitoring body to supervise the compliance with the codes of conduct, as well as to take appropriate safeguards in case of infringement. Likewise, the certification body must assume the responsibility to assess the participants' compliance with the certification criteria. Besides, the data controller or processor in the third country must make binding commitment to apply the appropriate safeguards. The enforcement problem of the co-cooperation is thus also addressed in the GDPR. Against this background, it can be concluded that the inherent problems represented by the co-regulation itself are taken into consideration, when the codes of conduct and certification mechanism are designed as legal bases for data transfers from the EU to a third country.

Nonetheless, it remains the fact that eligible codes of conduct and certification mechanisms are lacking on the market for the purpose of justifying data transfer from the EU to a third country, even though the GDPR has provided thresholds that meet at least partially the suggestions of the academic. The stakeholders seem to be still reluctant to actively contribute to the drafting and approval of the codes of conduct and certification mechanisms. Taken into consideration the challenges mentioned by the scholars concerning the general framework surrounding the co-regulation, including the positive and negative incentives, at least the following potential problems can be identified:

a. The ambiguousness of the data transfer rules

As demonstrated in the previous sections, the definition of "data transfer" from the EU to a third country is not by any means clarified in the GDPR. The case law of the CJEU does not shed much light on this subject either, since there are very few cases concerning this matter. It has been controversial in the literature for a long time, whether data transfers from the EU to a third country within the meaning of Chapter V GDPR also includes the transfer from an EU processor or an EU data subject to a third-country controller, who is subject to the GDPR per Art. 3 GDPR. Thus, data controllers in a third country face an ambiguous situation, this legal uncertainty will logically impede their motivation to comply with the data transfer rules under Chapter V GDPR.

Furthermore, the provisions concerning the codes of conduct and certification

mechanisms are not unambiguously designed either. For instance, with regard to codes of conduct that provide appropriate safeguards to data transfers from the EU to a third country, Art. 40 section 3 requires them to have general validity within the EU through an implementation act of the EU Commission. However, Art. 46 section 2 (e), which exclusively deals with the appropriate safeguards, only refers to "an approved code of conduct pursuant to Art. 40" without mentioning the general validity requirement. This leads to the controversy among the scholars, whether the existence of general validity is a compulsory condition for the codes of conduct to serve as an appropriate safeguard for data transfers from the EU to a third country.[549] Furthermore, the extra obligation imposed on the data importer in the third country, requiring them to make binding commitments to apply the appropriate safeguards as provided in Art. 46 section 2 (e) and (f), is open for different interpretations too. Questions can be raised such as, what kind of binding commitments should be made? between whom and/or to whom? Besides, the data controller or processor in the third country should make binding commitments to apply the "appropriate safeguards", does the "appropriate safeguards" mentioned here mean the codes of conduct and the certification mechanism itself? Or what should it mean? These questions are discussed in the literature, but no secure answers can be provided.

To address these problems, first, the EDPB should provide guidelines specifying the concept of the data transfer from the EU to a third country. Though the EDPB has already adopted several guidelines regarding some of the appropriate safeguards[550] and the derogations[551] within the framework of data transfer from the EU to a third country, these guidelines left the basic concept of data transfer untouched. Understandably, it might be the legislator's intention to leave this concept open for new circumstances and technologies, but the current lack of any solid standing point for interpreting this concept weakens the legal certainty of the GDPR and undermines the motivation of the

[549] For the general validity of the code of conduct being a necessary element: SCHRÖDER, Christian, Art. 46, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR – Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 10, 21, 35; SCHANTZ, Peter, Art. 46, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, p. 70. Against the general validity of the code of conduct being a necessary element: SCHWEINOCH, Martin, Art. 40, in: EHMANN, Eugen; SELMAYR, Martin, General Data Protection Regulation (Datenschutz-Grundverordnung). C.H.BECK, 2nd Edition 2018, p. 37.

[550] For example, Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted by the Art. 29 Working Party on 11 April 2018 and endorsed by the EDPB on 25 May 2018.

[551] EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25 May 2018.

data controllers and processors to comply with the data transfer rules. Now that the chance to make this move is passed with the promulgation of the GDPR, which leaves the problem unsolved, and the CJEU has not had many opportunities or probably also intention to clarify the matter, the EDPB should make use of its guiding function to shed at least some light on the matter.

Second, the EDPB should also issue guidelines clarifying the requirements for using codes of conduct and certification mechanisms to provide appropriate safeguard for data transfers as soon as possible, which was brought up by the EDPB a long time ago but has not become reality yet. In these guidelines, the aforementioned controversies and questions should be addressed.

b. The long-term neglect of enforcement of data transfer rules

Data transfer from the EU to a third country is a sensitive topic in the data protection realm, which should be preferably avoided and sealed from the perspective of the involved data controllers and processors. On the side of the data protection supervisory authorities, apart from the cases concerning giant American social media and search engine providers, investigation actions against data transfers concerning smaller data controllers and processors are rarely heard, which is not surprising due to the limited resources of the supervisory authorities. In other words, the chances for being sanctioned due to violation of the data transfer rules are rather slim. Meanwhile, drafting and monitoring the codes of conduct and certification mechanisms is associated with costs, both for the owner of the code (or the certification body) and for the data controllers or processors participating in it.[552] Such costs are not negligible, especially when the majority of the data controllers or processors involved are small or middle-sized enterprises. The poignant contrast of this uncertain, rather low probability of sanction and certain, visible costs may be one of the major reasons why incentives to draft codes of conduct and certification mechanisms are in lack, despite the benefices that codes of conduct and certification mechanisms could bring along.

In responding to these problems, based on further clarification of the concept of data

[552] See also KRANIG, Thomas; PEINTINGER, Stefan, Self-regulation in Data Protection Law in Germany, Europe and the USA, Taking into Account the Proposal for the GDPR (Selbstregulierung im Datenschutz-Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlages zur DS-GVO), ZD, 2014, p. 7.

transfer, the enforcement of the data transfer rules needs to be enhanced. It is well noted that the supervisory authorities have limited resources for conducting investigation and enforcement activities, and not many changes will happen to that in the foreseeable future. In view of this, a selective enforcement action in a certain period might be considered an option, as scholars have said, "it is enforceability that really matters, not actual enforcement".[553] Within the framework of data transfer from the EU to a third country, the supervisory authority is explicitly granted the power to order the suspension of data flows to a recipient in a third country,[554] in this sense, enforceability is not a major barrier for enforcing data transfer rules.

As for the costs that are associated with codes of conduct, there is already suggestion from scholars that the state should provide financial support for the drafting of codes of conduct, in particular at the very beginning.[555] In the China-EU cross-border E-Commerce context, as it is also in China's interest to facilitate data transfer from the EU to China, there should be space for the EU and China to establish joint projects in this area. Besides, the association or certification body that drafts and manages the code of conduct or certification mechanism should be allowed to charge an appropriate fee for the use of the code of conduct or certification. When determining the amount of such fee, the size of the majority of the involved data controllers or processors must be taken into consideration.

1.4 Derogations

Data controllers might also consider the derogations laid down in Art. 49 as legal bases for the intended data transfer. The reliance on derogations can be justified due to the practical unavailability of the appropriate safeguards.

However, as noted in the previous sections, the application of different derogations laid down in Art. 49 are subject to different conditions. Whereas consent of the data subjects

---

[553] KOHL, Uta, Jurisdiction and the Internet: Regulatory Competence over Online Activity. Cambridge University Press, Cambridge, 2007, p. 205.
[554] Art. 58 section 2 (j), GDPR.
[555] SPINDLER, Gerald; THORUN, Christian, The Role of Co-Regulation in the Information Society-Recommendation for Action on Digital Governance (Die Rolle der Ko-Regulierung in der Informationsgesellschaft-Handlungsempfehlung für eine digitale Ordnungspolitik), MMR-Beil, 2016, No. 6, p. 32.

could be relied upon also in regularly occurred circumstances, other derogations such as data transfer necessary for the performance of a contract or for the purpose of compelling interests pursued by the data controller are only limited to occasional, unsystematic data transfers. In the scenario of data transfer from an EU processor to a non-EU controller within the framework of cross-border E-Commerce, if the data transfer is necessary for the performance of the sales contract between the seller and the buyer or the service contract between the user and the E-Commerce platform, making use of the contract performance derogation might be an option at first sight. Nevertheless, since it can be assumed that there is a stable relationship between the processor and the controller, data transfers between these two parties are not to be considered occasional and unsystematic. Under such circumstances, the parties should always consider providing appropriate safeguards to the data subjects regarding their personal data.

The last option then remains to be the consent of the data subject. The data controller or processor must make sure that the strict conditions for an effective consent are met, as demonstrated above. Besides, the data controller or processor is inevitably exposed to the risk that if the data subject withdraws his or her consent, the transfer has to stop.

2. Data transfers from EU data subjects to Chinese controllers

In some other cases, Chinese sellers or service providers provide goods or services to EU consumers directly per internet and collect personal data in the same course. They have no data processor, no rented server, or any other facilities in the EU, so that the personal data are directly sent by the users to the data controllers established in China. As demonstrated in chapter 3 of this dissertation, such data flows should also be considered as data transfers from the EU to a third country. In such cases, there is no data controller or processor in the EU, the Chinese data controller alone has to ensure that the conditions under Chapter V GDPR for data transfers from the EU to third countries are met.

2.1 Applicability of the standard contractual clauses and binding corporate rules

It does not need much investigation to conclude that SCCs and binding corporate rules are not applicable to this scenario. SCCs are to be concluded between a data controller or processor within the EU and a data controller or processor in a third country. Though the number of the parties of the contractual clauses is not limited, in any event, there must be a data controller or processor in the EU. Likewise, for binding corporate rules to apply, there must be an enterprise within the EU that assumes liability for the processing activities of the enterprises outside of the EU, after the personal data are transferred. This is not the case if the data controller only resides in China. In short, any contractual mechanism that presupposes an intermediary in the EU, either a controller or processor, or an establishment of the Chinese controller in the EU, will not be applicable to the scenario discussed here.

2.2 Applicability of the codes of conduct and certifications

Given that the addressees of the codes of conduct and certifications are merely data controllers or processors in a third country, codes of conduct and certifications in principle match the characteristics of the scenario discussed here. Provided the Chinese data controller adheres to an approved code of conduct that is generally valid in the EU and makes binding and enforceable commitments to apply the code of conduct, or has its data processing operations certificated by an accredited certification body, it can transfer personal data to China lawfully. To that end, the code of conduct or certification mechanism must have taken into account the general legal conditions in China that are relevant to the data processing, in particular those illustrated in chapter 4 of this dissertation.

The problem of this approach is the same as that for data transfers from an EU processor to a non-EU controller, namely, neither is there any approved code of conduct that is partly or wholly directed at data transfers from the EU to a third country and declared general valid in the EU, nor certification mechanisms for that purpose.

2.3 Applicability of the derogations

Since the reliance on appropriate safeguards is currently impossible due to the inherent characteristics of the SCCs and binding corporate rules and the lack of valid code of conduct and certification mechanism, the data controller in China might also consider to base the data transfer on derogations laid down in Art. 49 GDPR. Which exact derogation may be relied upon to transfer the data to China is largely dependent on the individual circumstances of the data transfer.

2.3.1 Transfer is necessary for the performance of a contract

Within the framework of cross-border E-Commerce and in the scenario discussed here, the data controller is the seller or service provider located in China, while the data subject located in the EU is the visitor, user of the website or App hold by the data controller, and the potential buyer of the products provided by the data controller. Generally speaking, the data subject as user of the website or App might come into a contractual relationship with the data controller as seller or service provider in two circumstances. First, if the data subject registers with the website or App, a service (use) contract is generated between the data subject and the data controller concerning the use of the website or the App. Second, when the data subject purchases products or services on the website or App, a sales contract is concluded between the data subject and the data controller in terms of the purchase of the products or services. To fulfill these contracts, the seller or service provider as data controller might need to collect and transfer personal data to China. The transfer of such data can be based on the derogation, namely the data transfer is necessary for the performance of a contract between the EU data subject and the Chinese data controller. The literature generally considers this kind of transfer within the framework of E-Commerce as occasional and not repetitive.[556] Noteworthy is also that such data may only be used to fulfill the contract between the data subject and the data controller, any change of purpose must

[556] TOWFIGH, Emanuel V.; ULRICH, Jacob, Art. 4, in: SYDOW, Gernot, EU GDPR (Europäische Datenschutzgrundverordnung). Nomos, 2nd Edition 2018, p. 6; and SCHRÖDER, Christian, Art. 49, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR – FEDERAL DATA PROTECTION LAW (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 18.

base on another legal basis.

2.3.2 Consent of the data subject in the EU

Except for personal data that are necessary for the performance of a contract between the EU data subject and the Chinese data controller, when the EU users visit the website or App of the Chinese seller or service provider, their personal data might be collected automatically for other specified or not specified purposes, including for profiling and advertisement. The transfer of such data is not necessary for the performance of the contract between the data subject and the data controller; thus, the transfer needs another legal basis or has to meet the conditions of another derogation.

Another possible derogation that might fit in this scenario is the obtaining of the consent of the data subject. In this regard, the Chinese data controller has to keep in mind that the requirements imposed by Art. 49 section 1 (a) on the consent for data transfer from the EU to a third country are more stringent than that in the case of other data processing activities. The data subject must not only be given transparent information about the data processing and the data controller itself, but also the risks of the data transfer to China, that China has received no adequacy decision from the EU and no extra appropriate safeguards are provided by the data controller. The EDPB has noted in its guidelines that such notice about the risks of data transfer should also include detailed information such as whether there is a data protection supervisory authority in the third country, and whether the third country provides data protection principles and data subject rights.[557] Thus, the threshold on the "informed" consent in the case of data transfer is particularly high. On the basis of such transparent information, the data subject must give explicit consent separately on the specific data transfer, which means, the data subject must give an express statement, for example by a written statement, filling in an electronic form, sending an email or using an electronic signature.[558] The Art. 29 Working Party has noted in one of its Opinions which are later endorsed by the EDPB that, for E-Commerce, a data controller may obtain explicit consent by offering

[557] EDPB, Guidelines 2/2018 on derogations of Art. 49 under Regulation 2016/679, adopted on 25 May 2018, p. 8.
[558] EDPB, Guidelines 05/2020 on Consent under Regulation 2016/679, adopted on 4 May 2020, p. 18.

a Yes and No check boxes.[559] In the context of data transfers from the EU to China, such check box must specifically refer to the data transfer to China, instead of referring to a general data processing. Additionally, if the consent is obtained through standard clauses, such standard clauses have to be controlled in accordance with the relevant civil law provisions governing the standard clauses in each related Member State.

In the light of these highly strict conditions, in particular the detailed notice about the risks that the data subject is exposed to after the data transfer, it is very much doubtful whether the data subject would still give consent to the data transfer to China. Even if the data subject does give such explicit, specific consent, he or she may withdraw the consent anytime, even the EDPB indicates in its Guidelines that "consent might prove not to be a feasible long-term solution for transfers to third countries".[560]

III. Brief summary

This chapter investigates the feasibility to make use of the appropriate safeguards and derogations to transfer personal data from the EU to China within the China-EU cross-border E-Commerce framework. In general, the data transfers are classified into three scenarios and each of them are scrutinized in the light of the appropriate safeguards and derogations laid down in Art. 46 and Art. 49 GDPR.

In the scenario data transfer from an EU based data controller to a Chinese controller or processor, part I of this chapter analyzed the application of the SCCs to provide appropriate safeguard to data transfers in the "after Schrems II" era. Though the "Schrems II" judgement held the SCCs as a transfer tool valid, the requirements imposed on the data exporter and importer to assess the legal system of the third country and to adopt supplementary measures render the practical application of the SCCs extreme burdensome and risky. This is reflected in the scenario EU established cross-border platforms transferring personal data to Chinese sellers or service providers too. In the light of the "Schrems II" judgement, the data access by public authorities in China cannot be considered as limited to what is necessary and proportionate in a democratic

[559] Ibid.
[560] EDPB, Guidelines 2/2018 on derogations of Art. 49 under Regulation 2016/679, adopted on 25 May 2018, p. 8.

society. The question is, whether the data access by public authorities constitutes a realistic threat to the personal data transferred in the course of cross-border e-commerce. The author supports a risk-based approach as indicated in the Commission's New SCCs. Given that the personal data transferred during cross-border e-commerce usually do not belong to special categories of personal data and the purpose of the transfer is usually related to fulfilling the sales/service contract, the threshold for safeguarding these personal data should not be set too high. The assessment of the legal system in the third country should take into account the likelihood of the data access by public authorities, not the mere existence of a law that allows generalized access. An opposite position will just render the SCCs as a most frequently used transfer tool meaningless and leaves the most daily cross-border business activities relying on derogations which provide no extra protection to the data subjects or just slowly dying. If one follows this risk-based approach, the result would be, SCCs provide appropriate safeguard to the data transfer from the EU established cross-border e-commerce platforms to Chinese sellers, without the adoption of supplementary measures being necessary.

The circumstances relating to the scenario data transfer from an EU processor to a Chinese data controller are complicated too. The most frequently invoked type of appropriate safeguard, the Old SCCs that were issued by the Commission under the Data Protection Directive era, do not cover this scenario. The officially adopted New SCCs provides two new scenarios: data transfer from an EU processor to a non-EU controller and data transfer from an EU processor to a non-EU processor. However, it explicitly left out the scenario data transfer to a data importer that is subject to the GDPR per Art. 3 (2), in contrary to the Draft New SCCS. The author of this dissertation holds the opinion that module four "data transfer from processor to controller" should apply to transfers to a data importer that is already subject to the GDPR per Art. 3 (2). The author calls for the EDPB to shed more light on the concept of data transfer and on the question whether data flows to a data importer that is already subject to the GDPR per Art. 3 (2) constitute data transfers, and if yes, what kind of legal basis is available for such data transfers. Except for the SCCs, the GDPR's new introduced codes of conduct and certification mechanism as two types of co-regulation can theoretically also serve as an appropriate safeguard for the data transfer from the EU to a third country. These two approaches have the advantages to make use of the private bodies'

expertise and resources to unburden the public authorities, meanwhile provide more legal certainty to the stakeholders. However, the associations and certification bodies are still reluctant to draft codes of conduct and certification criteria after the promulgation of the GDPR. To provide more incentives for both the code provider and code user (the same applies to the certification provider and user), the author suggests to further clarify the basic concept of the data transfer and the preconditions for the codes of conduct and certification mechanisms to provide appropriate safeguards for data transfer. Besides, in order to push the smaller to middle-sized enterprises to take the data transfer rules under Chapter V GDPR seriously, more enforcement actions, even if selective ones, are needed in this area. Last but not least, states, in particular China and the EU for the relevance of this dissertation, should encourage relevant public-welfare foundations and associations in their own country to build joint projects to provide financial support and guidance for the co-regulation through codes of conduct and certification mechanisms, for this is both in the EU's interest to protect a fundamental right, and in China's interest to ensure smooth data transfer from the EU to China for the purpose of boosting cross-border E-Commerce.

As regard to the scenario data transfer directly from the EU data subject to the Chinese controller, chapter 3 of this dissertation argues that this scenario also belongs to data transfer within the meaning of Chapter V GDPR. In examining the applicability of the SCCs and binding corporate rules to this scenario, the chapter comes to the conclusion that any contractual mechanism that presupposes an intermediary in the EU, either a controller or processor, or an establishment of the Chinese controller in the EU, will not be applicable to the scenario discussed here. But just like in the previous scenario, codes of conduct and certification mechanism can cope with this scenario. The problem remains the same - there is no approved code of conduct or certification mechanism that is directed at providing appropriate safeguards for data transfer from the EU to a third country. Last, two derogations laid down in Art. 49 GDPR, namely the transfer is necessary for the performance of a contract and the consent of the data subject, are proved applicable to this scenario. However, the application of these derogations is restricted. The contract performance derogation only applies to personal data that is strictly necessary for the performance of a contract between the data subject and the data controller, which is usually merely part of the data collected and transferred by the

Chinese data controller. The processing of other personal data could be based on the consent derogation, however, in addition to the strict conditions imposed on the consent, the data subject can withdraw the consent at any time, which makes consent an instable legal basis for the data transfer.

Chapter 6 Summary and Conclusion

The boosting China-EU cross-border E-Commerce has generated massive transborder data flows from the EU to China. The most typical three scenarios arising from this business branch are the data flow from an EU based data controller to a Chinese controller or processor, the data flow from an EU processor to a Chinese controller, and the data flow from an EU data subject to a Chinese controller. This dissertation investigates on one side whether the GDPR, the EU's comprehensive data protection regulation, provides sufficient protection to the fundamental right of the EU data subjects, when their personal data are transferred from the EU to China. It examines on the other side whether the GDPR gives the data controller or processor involved in the data flow, in particular the data controller located in China, sufficient legal certainty by providing unambiguous, practically implementable rules to follow.

The rules in the GDPR that directly address the transborder data flow from the EU to a third country are Art. 3 which regulates the territorial application scope of the GDPR, and Chapter V that regulates data transfer from the EU to a third country. The question then further specifies as whether these two mechanisms of the GDPR, the territorial application scope and the rules concerning data transfer from the EU to a third country under Chapter V GDPR, provide sufficient protection to the natural persons in the EU concerning to their personal data, when such data are transferred outside of the EU.

The dissertation begins with a scrutiny of Art. 3, its application conditions and effects on the aforementioned three transborder data flow scenarios. Art. 3 stipulates in which circumstances the GDPR shall apply to the data processing activities. In general, the application scope of the GDPR is widely defined and further extended compared to the Data Protection Directive. First of all, for data controllers or processors that have an establishment in the EU, the GDPR applies to data processing activities that are carried out in the context of, or pursuant to the CJEU, "inextricably linked" to that EU establishment. Second, for data controllers or processors that do not have any establishment within the EU, or that establishment is not linked to the data processing activities carried out by such data controllers or processors, the GDPR will still apply to the data processing activities, if the data controllers or processors target their products or services at the EU data subjects or the data processing is carried out relating to such

provision of goods or services to the EU data subjects. This is called the "market place principle" in the literature, meaning the law of the targeted market should apply to the data processing operations. In addition, the GDPR also applies to data processing activities that are related to the monitoring of behaviors of the EU data subjects, for example by cookies. In this last circumstance, the element of "targeting" is not required as compared to the data processing related to the offering of products or services. Thus, the market place principle seems not to apply to this circumstance. This general application of the GDPR, going beyond the targeting approach, is partially accused by some scholars of being abundant and contradictive to the CJEU's case law explicitly stating that the EU data protection law should not apply universally.[561]

Against this background, the application scope of the GDPR is considered extraterritorial by scholars and commentators, some of which in a negative way.[562] After an examination of the jurisdiction and extraterritoriality concept, this dissertation comes to the conclusion that as regard to legislative and adjudicative jurisdiction, though it is commonly recognized that the territoriality principle (to be exact, the subjective territoriality principle) is the primary jurisdiction principle under public international law and also the most uncontroversial one, extraterritorial jurisdiction claims are not a rare phenomenon and can also find its basis in the various permissive jurisdiction principles under the Harvard Draft. However, it is well established under the public international law that enforcement jurisdiction is to a great extent territorial. It is uncontroversial that a state could only exercise enforcement jurisdiction on its own territory. This leads to a dilemma that a state may legislate extraterritorially but lacks the ability to enforce its law abroad. This is particularly true, when a state tries to regulate conducts of foreign persons or organizations who have neither organizational

[561] KLAR, Manuel, The Extraterritorial Effect of the New European Data Protection Law (Die extraterritoriale Wirkung des neuen Europäischen Datenschutzrechts). Datenschutz und Datensicherheit, 2017, Vol. 41, No. 9, p. 278-279.

[562] For example, AHMAD, Imran, Extraterritorial scope of GDPR: do Canadian businesses need to comply?, available at https://www.millerthomson.com/en/blog/mt-cybersecurity-blog/extraterritorial-scope-gdpr-canadian-businesses-need-comply/ last accessed on 18.09.2023; Herbert Smith Freehills, Extending the long arm of the law-extraterritoriality and the GDPR, available at https://www.herbertsmithfreehills.com/latest-thinking/extending-the-long-arm-of-the-law-extra-territoriality-and-the-gdpr; MOEREL, Lokke, the long arm of EU data protection law: does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?, International Data Privacy Law, 2011, Vol. 1, No. 1, p. 41; SVANTESSON, Dan Jerker B, The Extraterritoriality of EU Data Privacy Law - its Theoretical Justification and Its Practical Effect on US Businesses. Stanford Journal of International Law, 2014, Vol. 50, p. 60-73; SVANTESSON, Dan Jerker B, Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation. International Data Privacy Law, 2015, Vol. 5, pp. 226-234.

nor financial assets in the regulating state. Thus, the problem of the extraterritoriality of the GDPR lies rather in the enforcement difficulties since the data protection supervisory authority lacks the legal basis under public international law to enforce the law outside of the EU. This enforcement problem exists, not surprisingly, also in the EU-China interrelationship. Even though the data processing activities by the Chinese data controllers or processors would be subject to the GDPR, if the conditions laid down in Art. 3 GDPR are fulfilled, the enforcement of the GDPR in China faces significant challenges, either through public or private enforcement means. In this sense, the wide application scope of the GDPR per Art. 3 inherently has shortcomings in its enforceability, so that Art. 3 itself alone could not provide a satisfying protection to the EU data subjects, when their personal data are collected by data controllers or processors located outside of the EU.

The dissertation then goes on to examine whether Chapter V of the GDPR specifically regulating data transfer from the EU to a third country could compensate this shortcoming. This part commences with the attempt to figure out whether the definition of data transfer covers the transborder data flow scenarios focused in this dissertation. The definition of data transfer is not provided in the GDPR, nor does the case law of the CJEU and the guidelines of the EDPB shed much light on this matter. Chapter 3 of this dissertation tries to explain the data transfer concept from three aspects: first, the form of transfer, namely whether disclosures to certain recipients or uncertain recipients are considered data transfer; second, the intention of the transferor, namely whether the transferor should have the intention or at least the knowledge of the transferor that the personal data may be accessed by recipients in a third country; third, the identity of the transferor and the recipient. All three aspects are full of uncertainties, among which the identity of the transferor and the recipient is most closely related to the discussed scenarios here. The wording of Chapter V GDPR does not provide much elaboration about the identity of the transferor and the recipient, Art. 46 merely states that in the absence of an adequacy decision, a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, indicating that the transferor should be a controller or processor. However, it still leaves several questions open, such as whether the exporting controller or processor must be located within the EU, since according to Art. 3 section

2 GDPR, under certain circumstances non-EU data controllers can be subject to the GDPR too. Another question is when the data exporter is a processor, does chapter V GDPR only applies to the data transfer from that exporting processor to a sub-processor or also to a non-EU controller. Further, it is somewhat controversial too whether the data subject itself could act as an exporter to transfer its own data outside of the EU. Thus, it is uncontroversial that Chapter V GDPR applies when a EU data controller or processor transfers personal data to a non-EU data controller or processor that is not subject to the GDPR per Art. 3. What unclear at the current stage is, whether the other two scenarios discussed in this dissertation, namely data flows from an EU data processor to a non-EU data controller that is subject to the GDPR per Art. 3, and that from the data subject to a non-EU data controller that is subject to the GDPR per Art. 3, constitute a data transfer to a third country within the meaning of Chapter V of the GDPR. Scholarly opinions concerning these questions are pretty much controversial and wavering. Scholars against this interpretation mainly have two arguments, first, if the data controller in the third country is already subject to the GDPR per Art. 3, then the fundamental right of the EU data subjects to data protection will not be undermined, since the controller in the third country has to comply with the GDPR just as any EU data controller.[563] Second, if Chapter V is to apply to the circumstance in which personal data are transferred from the EU to a data controller located in a third country but subject to the GDPR per Art. 3, such transfer has to be based on a legal basis laid down in Chapter V, however, at the current stage, there is no appropriate safeguard applicable to this circumstance, at least not for the data subject - data controller scenario.[564] In that regard, this dissertation argues that the concept of data transfer should be construed broadly to cover the circumstance in which personal data are transferred from the EU to a data controller that is located in a third country but subject to the GDPR per Art. 3. With regard to the argument, that if the data controller in the third country is already subject to the GDPR per Art. 3, the fundamental right of the EU data subjects to data protection will not be undermined, chapter 2 of this dissertation analyzing the extraterritoriality of the GDPR has already pointed out the enforcement

[563] For example, SIMITS, S.; HORNUNG, G.; SPIECKER gen. DÖHMANN, I. Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, Art. 44, p. 14, citing KUNER, Christopher. Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law. International Data Privacy Law, 2015, Vol.5, pp. 235-245.

[564] See SCHANTZ, Peter, Art. 44, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht), Nomos, 1st Edition 2019, pp. 12-16.

problem of a wide application of the GDPR to data controllers and processors located outside of the EU. It has come to the conclusion that due to the enforcement difficulties and other problems resulted from the location of the personal data in the third country, Art. 3 GDPR alone is not able to provide a sufficient level of protection of personal data in a third country. It makes sense to combine Art. 3 and the data transfer rules laid down in Chapter V GDPR in order to achieve a better protection of personal data of the EU data subjects in the third country.

Following this logic, if Chapter V GDPR is to apply to the circumstance in which personal data are transferred from the EU to a data controller that is located in a third country but subject to the GDPR per Art. 3, chapter 4 and 5 of this dissertation then further examine whether there is at least a legal basis under Chapter V GDPR to justify the three data transfer scenarios discussed in this dissertation. Since relying on an adequacy decision is the most secure and convenient way for any kind of data transfer from the EU to a third country, chapter 4 first conducts an assessment of the Chinese data protection level, in order to explore whether, with the quick progress made to the data protection law in China in the last few years, an adequacy decision regarding China is possible with the rapid development in data protection in China, in particular with the promulgation of the PIPL. After analyzing the data protection provisions in the Cybersecurity Law and its specifications, the Civil Code and the PIPL, chapter 4 comes to the conclusion that the substantial data protection rules in China are in principle comparable to those of the GDPR in terms of the data processing principles, the rights of the data subject and the obligations of the data controller and processor. The flaws lie mainly in the lack of an effective regulation of the data processing activities by public authorities and an independent data protection supervision authority both for the private and the public sector, leading to an insufficient supervision of the compliance and implementation of the substantial rules in the practice. The data subject in principle has a right to lodge a complaint to the competent supervisory authority, however, there is no independent data protection supervisory authority in China. In the Cybersecurity Law and the PIPL, the competent authority that is responsible for the protection of personal data and supervision of the data protection rules is the “cyber space administration and other relevant ministries within their own functions and competences”. This uncertainty in terms of the determination and competence of the

competent supervision authority impedes the practical implementation of the right to administrative remedy. In terms of judicial remedy, the Civil Code and the Administrative Procedural Law generally allow natural persons to file a civil proceeding against private data controllers or processors and administrative proceeding against public data controllers or processors. Whereas civil proceedings in this area experienced a rise in the last few years along with the introduction of data protection provisions in various laws, administrative proceeding against public authorities due to unlawful data processing, in particular over-collection and sharing of personal data barely exists. This again reveals that the regulation of data processing by public authorities is theoretically ill-designed and practically of no significance in China. Last, the access of public authorities for criminal law enforcement and national security purposes is largely unrestricted and the concerned data subject has little chance to challenge the data processing in administrative and judicial means. In the light of these analysis and the "Schrems II" judgement, it must be concluded that the current data protection law together with the surrounding legal system in China does not ensure an equivalent level compared to that in the EU, an adequacy decision concerning China is even with the promulgation of the new comprehensive data protection law rather unlikely, since the mechanism concerning the implementation and supervision of the substantial data protection rules remains largely unchanged and the excessive access of personal data by public authorities for criminal law enforcement and national security purposes is not addressed at all. If China wishes to seriously be considered as a candidate of an adequacy decision, a more comprehensive, systematic reform in the whole data protection relevant system would be necessary, this is not only to mean the substantial data protection law itself, but more the ecosystem that ensures the effective implementation of such rules in the practice. Further, changes also need to be taken in other law areas such as in the Criminal Procedure Law and the National Security Law to lift up the data protection level in those areas to match the whole picture.

Chapter 5 then further examines whether other appropriate safeguards laid down in Chapter V GDPR and the derogations can justify the data transfer from the EU to China in the three scenarios discussed in this dissertation. In the first scenario, namely for data transfer from an EU data controller to a Chinese data controller or processor, the SCCs appear to be an appropriate transfer tool at first look. A genuine obstacle of transferring

the personal data to China based on the SCCs in this scenario is, however, as analyzed and concluded in the previous chapter 4 of this dissertation, that the Chinese laws grant the intelligence authorities and criminal law enforcement authorities access to personal data without defining the scope and conditions of such data access clearly and precisely, and that the data subjects are not granted with actionable rights and effective legal remedy regarding such data access by public authorities. In the light of the "Schrems II" judgment, this kind of access cannot be considered as limited to what is necessary and proportionate in a democratic society. The question is, whether the data access by public authorities constitutes a realistic threat to the personal data transferred in the course of cross-border e-commerce. The author supports a risk-based approach as indicated in the Commission's New SCCs. This means, for data transfer in the context of cross-border e-commerce, the assessment of the legal system in the third country should take into account the likelihood of the data access by public authorities, not the mere existence of a law that allows generalized access. Given that no news or reported precedents regarding personal data access requests made by public authorities against cross-border e-commerce operators has been found, if one follows this risk-based approach, the result would be, SCCs provide appropriate safeguard to the data transfer from the EU established cross-border e-commerce platforms to Chinese sellers, without the adoption of supplementary measures being necessary. It must be stressed again that one has to take into account the nature and the amount of the data to be transferred and the purpose of the transfer, before accessing whether the mere existence of a law that allows generalized access already constitutes a realistic threat to the data transferred. On the contrary, if one does not follow this risk-based approach, the result would be that the SCCs do not provide adequate protection to the personal data transferred due to the existence of laws allowing generalized data access by public authorities in China. As a consequence, the controller in the EU must take supplementary measures to mitigate the influence of such laws. However, according to the EDPB's Recommendation on Supplementary Measures, no supplementary measures are able to compensate this situation, and the data transfer from a EU controller to a Chinese controller or processor must be ceased. In the context of the cross-border e-commerce, this means the e-commerce platform operators established in the EU cannot transfer personal data of EU data subjects to Chinese sellers or service providers. Practically, this would put an end to the China-EU cross-border e-commerce per big e-commerce

platforms such as Amazon, eBay or Wish.

For the other two scenarios, there are no effective SCCs tailored to these two scenarios. Besides, the binding corporate rules only apply to data transfers within big corporation groups, its application scope is thus inherently limited. The officially adopted New SCCs cover two new scenarios: data transfer from an EU processor to a non-EU controller and data transfer from an EU processor to a non-EU processor. However, it explicitly left out the scenario data transfer to a data importer that is subject to the GDPR per Art. 3 (2), in contrary to its previously published Draft New SCCs for public consultation. The author of this dissertation holds the opinion that module four "data transfer from processor to controller" should apply to transfers to a data importer that is already subject to the GDPR per Art. 3 (2). The author calls for the EDPB to shed more light on the concept of data transfer and on the question whether data flows to a data importer that is already subject to the GDPR per Art. 3 (2) constitute data transfers, and if yes, what kind of legal basis is available for such data transfers. Another possibility that deserves more attention both from the regulators and the stakeholders is the co-regulation options that serve as appropriate safeguards for data transfers from the EU to a third country, namely the codes of conduct and data protection certification mechanism. These two options have the advantage that they are addressed at the data controller or processor in the third country, thus no data controller or processor as intermediary in the EU is required. This is the only chance for the third scenario - data transfer directly from the EU data subject to the Chinese controller. In addition, these two mechanisms also have another advantage of making use of the private bodies' expertise and resources to unburden the public authorities. The monitor body of a code of conduct, which is an independent body and has expertise in the data protection field, monitors the compliance with the code of conduct. The monitoring body also has the competence to take appropriate actions in cases of infringement of the codes of conduct, including contractual penalties. For codes of conduct that aim at providing appropriate safeguards for data transfers to third countries, the monitor body must be in the position to monitor the compliance by controllers or processors in the third country that adhere to it and enforce sanctions directly in the third country where the data controller locates. This is an inherent requirement for codes of conduct that are drafted for the purpose of providing appropriate safeguards for data transfers to third countries, and it is exactly

this feature that makes codes of conduct a better enforcement tool than "hard enforcement" by data protection supervisory authorities or judgements of the EU courts. The same also applies to the certification mechanisms. The certification body has to monitor the compliance of the controller or processor in the third country with the GDPR according to the certification criteria, if the processing activities of the controller or processor in the third country no longer meet the certification criteria, the certification must be withdrawn. In conclusion, the monitoring body and certification body has more resources and a more recognizable contractual legal basis to conduct supervision and enforcement against the data controller established in the third country.

Despite all the above-mentioned advantages, the problem of the codes of conduct and certification mechanism is the stakeholder's lack of incentive to draft and apply them in the practice. This can be attributed to the ambiguousness of the data transfer rules, the neglect of their enforcement and the costs associated with the implementation of the codes of conduct and certification mechanisms. This dissertation thus calls for more guidance and legal certainty from the EU level concerning the concept of data transfer and the precise application conditions for the codes of conduct and certification mechanism for the purpose of providing appropriate safeguard for data transfer from the EU to a third country. In terms of the neglect of the enforcement of the data transfer rules, the author supports the opinion that selective enforcement against small and middle-sized data controllers or processors might be a realistic way to transform the data transfer rules from paper to reality. As regard to the costs associated with it, the author holds that the association or the certification body should be allowed to charge a reasonable management fee from the data controller or processor. Besides, there is space for the EU and China to build joint projects for drafting and managing codes of conduct or certification mechanism for the purpose of transferring personal data from the EU to China, since the EU has an interest to protect its natural persons fundamental right, and China has an interest to expand its cross-border E-Commerce business in the EU.

To sum up, in the current stage, the huge uncertainties around the concept and legal basis of data transfer from the EU to a third country leaves the transborder data flows from the EU to China largely unregulated. Even the data exporter and the data importer are in good faith, the lack of options in terms of legal basis for data transfers, caused

either by the highly strict requirements set out by the CJEU in “Schrems II” for SCCs or by the practical unavailability of the codes of conduct and certification mechanisms, makes it extremely difficult and little attractive for them to carry out data transfers in full compliance with the GDPR. This situation is in urgent need of improvement both from the EU and China legislators.

From the EU side, if the EU requires that personal data transferred to a third country continue enjoying a level of protection essentially equivalent to that of the EU, it should make this practically possible by defining the data transfer concept clearly and providing implementable transfer tools as legal basis, as suggested above.

From the Chinese side, the PIPL has just come into force, detailed implementing rules and standards are under preparation intensively, China has the chance to draw its data protection level closer to the EU standard comprehensively, during which the factors necessary for the assessment of the data protection level in a third country must be taken into consideration. In addition to the PIPL, more importantly, changes also need to be taken in other law areas such as in the Criminal Procedure Law and the National Security Law to lift up the data protection level in those areas to match the whole picture.

By doing so, even if an adequacy decision regarding China will not come into sight in the near future, the threshold set out by the “Schrems II” judgement for appropriate safeguards might be easier for the parties to achieve. Otherwise, a huge gap in data protection level will only add more unstable elements into the EU-China trade, which already suffers from legal, cultural and political divergences between the EU and China. Due to China’s roll as a major exporting party in the cross-border e-commerce area, China might have even more to lose than the EU if such gap in data protection level ultimately ends up in suspension of the EU-China data transfer and shrink of the China-EU cross-border e-commerce.

Bibliography

I. Literature

ANTONIOU, Giannakis; BATTEN, Lynn, E-Commerce: Protecting Purchaser Privacy to Enforce Trust. Electronic Commerce Research, 2011, Vol. 11, pp. 421-456.

BENNETT, Colin; ODURO-MARFO, Smith, Global Privacy Protection: Adequate Laws, Accountable Organizations and/or Data Localization? Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers, 2018, p. 881.

BERGT, Matthias, Rules of Conduct as a Means of Eliminating Legal Uncertainty in the General Data Protection Regulation (Verhaltensregeln als Mittel zur Beseitigung der Rechtsunsicherheit in der Datenschutz-Grundverordnung). Computer und Recht, 2016, Vol.32, No. 10, p. 673.

BERGT, Matthias, The Importance of Codes of Conduct and Certification under the General Data Protection Regulation (Die Bedeutung von Verhaltensregeln und Zertifizierungen nach der Datenschutz-Grundverordnung). Smart World-Smart Law, 2016, pp. 483-499.

BERGT, Matthias; PESCH, Paulina Jo, Art. 40, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR – FEDERAL DATA PROTECTION LAW (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 22.

BORGES, Georg, Chapter 3, in: HELFRICH, Marcus; FORGÓ, Nikolaus; SCHNEIDER, Jochen, Operational Data Protection (Betrieblicher Datenschutz). C.H.BECK, p. 50.

BRAUNECK, Jens, Market Place Principle of the GDPR: Global Validity for EU Data Protection (Marktortprinzip der DSGVO: Weltgeltung für EU-Datenschutz?) EuZW, 2019, No. 12, pp. 496-497.

BRKAN, Maja, Data Protection and European Private International Law: Observing a Bull in a China Shop. International Data Privacy Law 2015, Vol. 5, No. 4, pp. 257-278.

BRKAN, Maja, The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core. European Constitutional Law Review, 2018, Vol. 14, No. 2, pp. 332-368.

BUCHNER, Benedikt; PETRI, Thomas, Art. 6, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR – Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition, 2020, p. 83.

BYGRAVE, Lee A, Data Privacy Law: An International Perspective. Oxford University Press, Oxford, 2014.

BYGRAVE, Lee A, Privacy and Data Protection in an International Perspective. Scandinavian studies in law, 2010, Vol. 56, pp. 165-200.

CAI, Jun (蔡军), Analysis of the Legislation of the Crime of Infringing Personal Information - on the Reflection and Prospect of the Crime Legislation（侵犯个人信息犯罪立法的理性分析—兼论对该罪立法的反思与展望). Modern Law Science (现代法学), 2010, Vol. 32, p. 105-112.

Centre for Information Policy Leadership White Paper, Essential Legislative Approaches for Enabling Cross-border Data Transfers in a Global Economy, 25 September 2017.

Centre for Information Policy Leadership White Paper, Essential Legislative Approaches for Enabling Cross-border Data Transfers in a Global Economy, 25 September 2017.

CHANDER, Anupam, Is Data Localization a Solution for Schrems II? Journal of International Economic Law, 2020, No. 3, pp. 771-784.

CHEN, Yu-Jie; LIN, Ching-Fu; LIU, Han-Wie, Rule of Trust: The Power and Perils of China's Social Credit Megaproject. Columbia Journal of Asia Law, 2018, Vol. 32, No. 1, p. 1, 27.

CHENG, Xiao (程啸), On the Nature of Personal Information Rights and Interests in the Civil Code (论我国民法典中个人信息权益的性质). Political Science and Law (政治与法律), 2020, Vol. 8, pp. 2-14.

CHENG, Xiao (程啸), Personal Information Protection from the Perspective of the codification of the Civil Code (民法典编纂视野下的个人信息保护). China Legal Science (中国法学), 2019, Vol. 4, pp. 26-43.

CRAWFORD, James, Brownlie's Principles of Public International Law. Oxford University Press, Oxford, 2019.

DE HERT, Paul; CZERNIAWSKI, Michal, Expanding the European Data Protection Scope Beyond Territory. International Data Privacy Law, 2016, Vol. 6, No. 3, pp. 240-241.

DEMARY, Vera, et al, Data Sharing im E-Commerce— Legal and Economic Basics (Rechtliche und ökonomische Grundlagen). Gutachten für ServiCon Service & Consult eG, 2019.

DLA Piper, DLA Piper Comments on EDPB Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data (Public Consultation Reference R01/2020), 21 December 2020.

DODGE, William S, Breaking the Public Law Taboo. Harvard International Law Journal, 2020, Vol. 43, p. 161.

ERNST, Stefan, Art. 4, in: PAAL, Boris P.; PAULY, Daniel A, GDPR - Federal Data Protection Act (DS-GVO BDSG). C.H.BECK, 3rd Edition 2021, p. 57.

ESAYAS, Samson Yoseph, A walk in to the Cloud and Cloudy It Remains: The Challenges and Prospects of "Processing" and "Transferring" Personal Data. Computer Law & Security Review, 2012, Vol. 28, No. 6, p. 670.

European Commission, Directorate-General for Justice and Consumers, BODEA, G., STUURMAN, K., BREWCZYŃSKA, M. et al., Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679 – Final report, Publications Office, 2019, European Federation of Data Protection Officers, Comments on the EDPB Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, 22 December 2020.

FRENZEL, Eike Michael, Art. 82, in: PAAL, Boris P.; PAULY, Daniel A, GDPR - Federal Data Protection Act (DS-GVO BDSG). C.H.BECK, 2nd Edition 2018, p. 6.

GABEL, Detlev, Art. 44, in: TAEGER, Jürgen; GABEL, Detlev, GDPR-German Data Protection Act (DSGVO-BDSG). Specialist Media Law and Economics, 3rd Edition 2019, p.10, 38.

GABEL, Detlev, Art. 47, in: TAEGER, Jürgen; GABEL, Detlev, GDPR-German Data Protection Act (DSGVO-BDSG). Specialist Media Law and Economics, 3rd Edition 2019, p. 2.

GABEL, Detlev, German Data Protection Act old version (BDSG aF) § 4 c, in: TAEGER, Jürgen; GABEL, Detlev, GDPR-German Data Protection Act (DSGVO-BDSG). Specialist Media Law and Economics, 3rd Edition 2019, p. 27.

GAO, Fuping (高富平), Personal Information Protection: From Personal Control to Social Control (个人信息保护：从个人控制到社会控制). Chinese Journal of Law (法学研究), 2018, Vol. 40, p. 18.

GEISSLER, Dennis; STRÖBEL, Lukas, Claims for Damages Under Data Protection Law in the Model Determination Procedure (Datenschutzrechtliche Schadensersatzansprüche im Musterfeststellungsverfahren). NJW, 2019, No. 47, pp. 3414-3418.

GOLDSMITH, Jack, Unilateral Regulation of the Internet: A Modest Defence. European Journal of International Law. 2000, Vol. 11, No. 1, pp. 135-148.

GREENLEAF, Graham, The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108. International Data Privacy Law 2012, Vol. 2, No. 2, pp. 68-92.

GREZE, Benjamin, The Extraterritorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives. International Data Privacy Law, 2019, Vol. 9, pp. 109-128.

HAN, Dayuan (韩大元), The Origin and Evolution of the Concept of Fundamental Rights in China (基本权利概念在中国的起源与演变). China Legal Science (中国法学), 2009, Vol. 6, p. 11, 23-25.

HÄRTING, Niko, GDPR (Datenschutz-Grundverordnung). Otttoschmidt, 2016, p. 234.

HERBST, Tobias, Art. 4 (2), in: KÜHLING, Jürgen; BUCHNER, Benedikt. GDPR – FEDERAL DATA PROTECTION LAW (DS-GVO/BDSG). C.H. BECK, 2nd Edition 2018, pp. 30-31.

HON, W. Kuan; MILLARD, Christopher, Data Export in Cloud Computing-How Can Personal Data Be Transferred outside the EEA: The Cloud of Unknowing, Part 4. SCRIPTed, 2012, Vol. 9, p.25.

HON, W. Kuan; MILLARD, Christopher, Data Exports in Cloud Computing-How Can Personal Data be Transferred outside the EEA? The Cloud of Unknowing. Queen Mary School of Law Legal Studies Research Paper 2011, No. 85, pp. 34, 35.

HORNUNG, Gerrit, Art. 3, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht). Nomos, 1st Edition 2019, pp. 34, 50.

Introductory Comment to the Draft Convention on Jurisdiction with Respect to Crime. American Journal of International Law, 1935, Vol. 29, pp.442-445.

JIANG, Yong (蒋勇), The Procedural Law Change of China's Electronic Evidence Collection Rules From the Perspective of Personal Information Protection (个人信息保护视野下中国电子取证规则的程序法转向). Journal of Xi'an Jiaotong University (西安交通大学学报), 2019, Vol. 39, No. 6, p. 9, 144.

Joint Comments by SRIW, Scope Europe and the EU Cloud Code of Conduct, Comments on EDPB Public Consultation R01/2020: 'Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data', December 2020.

JUNGKIND, Art. 40, in: WOLFF, Heinrich Amadeus; BRINK, Stefan; UNGERN-STERNBERG, Antje v., BeckOK Data Protection Law (Datenschutzrecht). BeckOK Online-Commentary, 35. Edition, p. 26.

KAMMINGA, Menno, Extraterritoriality. Max Planck Encyclopedias of International Law, 2012, pp. 1070-1077.

JUAREZ, Tavares, Art. 44, in: WOLFF, Heinrich Amadeus; BRINK, Stefan; UNGERN-STERNBERG, Antje v., BeckOK Data Protection Law (Datenschutzrecht).

BeckOK Online-Commentary, 44. Edition, p. 15.

KLAR, Manuel, The Extraterritorial Effect of the New European Data Protection Law (Die extraterritoriale Wirkung des neuen Europäischen Datenschutzrechts). Datenschutz und Datensicherheit, 2017, Vol. 41, No. 9, p. 278, 279, 536.

KLAR, Manuel, Art. 3, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR – Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, pp.25-51.

KLAR, Manuel, Art. 3, in: KÜHLING, Jürgen; BUCHNER, Benedikt. GDPR – FEDERAL DATA PROTECTION LAW (DS-GVO/BDSG). C.H. BECK, 3nd Edition 2020, p. 38.

KOHL, Uta, Jurisdiction and the Internet: Regulatory Competence over Online Activity. Cambridge University Press, Cambridge, 2007, p. 205.

KRANIG, Thomas; PEINTINGER, Stefan, Self-regulation in Data Protection Law in Germany, Europe and the USA, Taking into Account the Proposal for the GDPR (Selbstregulierung im Datenschutz-Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlages zur DS-GVO). ZD, 2014, pp. 3-9.

KUNER, Christopher, European Data Privacy Law and Online Business. Oxford University Press, Oxford, 2003.

KUNER, Christopher, Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law. International Data Privacy Law, 2015, Vol.5, pp. 235-245.

KUNER, Christopher, The European Union and the search for an international data protection framework. Groningen Journal of International Law, 2014, Vol. 2, pp. 55-71.

KUNER, Christopher, Transborder Data Flows and Data Privacy Law. Oxford University Press, Oxford, 2013.

KUNER, Christopher, Art. 44, in: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher. The EU Data Protection Regulation (GDPR): A Commentary. Oxford University Press, Oxford, 1st Edition 2020, p. 1153;

LANGE; FILIP, Art. 46, in: WOLFF, Heinrich Amadeus; BRINK, Stefan; UNGERN-STERNBERG, Antje v., BeckOK Data Protection Law (Datenschutzrecht). BeckOK Online-Commentary, 35. Edition, p. 10, 29.

LAUE, Philip, § 8 Self-Regulation (Selbstregulierung), in: LAUE, Philip; KREMER, Sascha, The New Data Protection Law in Business Practice (Das Neue Datenschutzrecht in der Betrieblichen Praxis). 2nd Edition 2019, p. 9.

LEE, Jyh-An, Hacking into China's Cybersecurity Law. Wake Forest Law Review, 2018, Vol. 53, p. 57, 88.

LENAERTS, Koen, Limits on Limitations: The Essence of Fundamental Rights in the EU. German Law Journal, 2019, No. 6, pp. 779-793.

LEPPERHOFF, Niels, Arts. 40 and 41, in: GOLA, Peter; HECKMANN, Dirk, Commentary on the GDPR – Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 2nd Edition 2018, p. 9, 22.

LI, Liang (李亮), Inspection and Exploration of Personal Information Protection in the New Criminal Procedure Law (新刑事诉讼法中个人信息保护的检视与路径探索). Humanities & Social Sciences Journal of Hainan University (海南大学学报人文社会科学版), 2014, No. 2, pp. 88-97.

LIANG, Huixing (梁慧星), Understanding and Application of the Important Provisions in "General Provisions of Civil Law" (《民法总则》重要条文的理解与适用). Journal of Sichuan University (四川大学学报), 2017, No. 4, pp. 51-65.

LINDSAY, David, Website Blocking Injunctions to Prevent Copyright Infringements: Proportionality and Effectiveness. The University of New South Wales Law Journal, 2017, Vol. 40, p. 1507.

LIU, Xianquan (刘宪权); FANG, Jinye (方晋晔), Legislation and Perfection of Criminal Law Protection of Personal Information Right (个人信息权刑法保护的立法及完善). Journal of East China University of Political Science and Law (华东政法大学学报), 2009, No. 3, pp. 120-130.

LONG, Weiqiu (龙卫球); LIU, Baoyu (刘保玉), Guidance for Interpretation and Application of the General Provisions of the Civil Law of the People's Republic of China (中华人民共和国民法总则释义与适用指导). China Legal Publishing House (中国法制出版社), 2017, p. 404.

LUNDSTEDT, Lydia, International Jurisdiction over Crossborder Private Enforcement Actions under the GDPR. Stockholm University Research Paper, 2018, No. 57.

MA, Mingfei (马明飞); CAI, Siyang (蔡斯扬), The Reciprocity Principle in the Recognition and Enforcement of Foreign Judgments in China (我国承认与执行外国判决中的互惠原则). Political Science and Law (政治与法律), 2019, Vol. 3, P. 14.

MILANOVIC, Marko, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age. Harvard International Law Journal, 2015, Vol. 56, p. 81.

MILLARD; KAMARINGOU, Art. 28, in: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher, The EU Data Protection Regulation (GDPR): A Commentary. Oxford University Press, Oxford, 1st Edition 2020, pp. 948-949.

MILLS, Alex, Rethinking Jurisdiction in International Law. British Yearbook of International Law, 2014, Vol. 84, pp. 187-239.

MOEREL, Lokke, The Long Arm of EU Data Protection Law: Does the Data Protection

Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide? International Data Privacy Law, 2011, Vol. 1, No. 1, pp. 28-46.

PATO, Alexia, The Collective Private Enforcement of Data Protection Rights in the EU. available at SSRN 3303228.

PAULY, Daniel A, Art. 44, in: PAAL, Boris P.; PAULY, Daniel A, GDPR - Federal Data Protection Act (DS-GVO BDSG). C.H.BECK, 3rd Edition 2021, pp. 1-5.

PAULY, Daniel A, Art. 46, in: PAAL, Boris P.; PAULY, Daniel A, GDPR - Federal Data Protection Act (DS-GVO BDSG). C.H.BECK, 3rd Edition 2021, pp. 21, 34-36.

PAULY, Daniel A, Art. 47, in: PAAL, Boris P.; PAULY, Daniel A, GDPR - Federal Data Protection Act (DS-GVO BDSG). C.H.BECK, 3rd Edition 2021, p.4.

PAULY, Daniel A; KUMKAR, Lea Katharina, Art. 40, in: PAAL, Boris P.; PAULY, Daniel A, GDPR Federal Data Protection Act (DS-GVO BDSG). C.H.BECK, 3rd Edition 2021, p. 9a.

QI, Aimin (齐爱民), Model Law on the Personal Information Protection Law (Scholar Draft) (中华人民共和国个人信息保护法示范法草案学者建议稿). Hebei Law Science (河北法学), 2005, No. 6, pp. 2-5.

REICHEL, Jane; CHAMBERLAIN, Johanna, The Relationship Between Damages and Administrative Fines in the EU General Data Protection Regulation. Faculty of Law, Stockholm University Research Paper, 2019, No. 72.

REIMER, Philipp, Art. 4, in: SYDOW, Gernot, EU GDPR (Europäische Datenschutzgrundverordnung). Nomos, 2nd Edition 2018, pp. 68-70.

ROSSNAGEL, Alexander, Art. 40, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht). Nomos, 1st Edition 2019, pp. 51-54.

RYNGAERT, Cedric, Jurisdiction in International Law. Oxford University Press, Oxford, 2015.

SAMIE, Najeeb, The Doctrine of" Effects" and the Extraterritorial Application of Antitrust Laws. Lawyer of the Americas, 1982, Vol. 14, No. 1, pp. 23-59.

SCHANTZ, Peter, Art. 44, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht). Nomos, 1st Edition 2019, pp. 12-16.

SCHANTZ, Peter, Art. 46, in: SIMITS, Spiros.; HORNUNG, Gerrit; SPIECKER gen. DÖHMANN, Indra, Data Protection Law (Datenschutzrecht). Nomos, 1st Edition 2019, p. 8, 32, 67-70.

SCHLINK, Bernhard, The Right of Informational Self-determination (Das Recht der

informationellen Selbstbestimmung). Der Staat, 1986, Vol. 25, p. 233.

SCHÖTTLE, Hendrik, III. Internationaler Datentransfer, in: WETH, Stephan; HERBERGER, Maximilian; WÄCHTER, Michael, Data and Personality Protection in the Employment Relationship (Daten- und Persönlichkeitsschutz im Arbeitsverhältnis). C.H.BECK, 2nd Edition 2019, p. 14

SCHRÖDER, Christian, Art. 44, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR – Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 16.

SCHRÖDER, Christian, Art. 46, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR – Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 10, 21, 35.

SCHRÖDER, Christian, Art. 47, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR – Federal Data Protection Law (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 13.

SCHRÖDER, Christian, Art. 49, in: KÜHLING, Jürgen; BUCHNER, Benedikt, GDPR – FEDERAL DATA PROTECTION LAW (DS-GVO/BDSG). C.H. BECK, 3rd Edition 2020, p. 18.

SCHWARTZ, Paul M, Information Privacy in the Cloud. University of Pennsylvania Law Review, 2012, Vol. 161, p. 1623.

SCHWEINOCH, Martin, Art. 40, in: EHMANN, Eugen; SELMAYR, Martin, General Data Protection Regulation (Datenschutz-Grundverordnung). C.H.BECK, 2nd Edition 2018, p. 37, 52.

SHANG, Xixue Shang (商希雪), Personal Data Sharing beyond Civil rights- An Analysis Based on the Legitimate Interests in the GDPR (超越私权属性的个人信息共享-基于《欧盟一般数据条例》正当利益条款的分析). Studies in Law and Business (法商研究), 2020, Vol. 37, No. 2, pp. 57-70.

SONG, Yahui (宋亚辉), Research on Private Law Protection Mode of Personal Information—An Interpretation Theory of Article 111 of the "General Provisions of Civil Law" (个人信息的私法保护模式研究-《民法总则》第 111 条的解释论). Journal of Comparative Law (比较法研究), 2019, No. 2, pp. 86-103.

SPINDLER, Gerald, Data Protection and Privacy Rights on the Internet-the Framework for Research Tasks and Need for Reform (Datenschutz- und Persönlichkeitsrechte im Internet-der Rahmen für Forschungsaufgaben und Reformbedarf). GRUR, 2013, No. 10, p.1003.

SPINDLER, Gerald; THORUN, Christian, The Role of Co-Regulation in the Information Society-Recommendation for Action on Digital Governance (Die Rolle der Ko-Regulierung in der Informationsgesellschaft-Handlungsempfehlung für eine

digitale Ordnungspolitik). MMR-Beil, 2016, No. 6, pp. 1-32.

SUN, Ping (孙平), Systematic Construction of the Fundamental Right Model of Personal Information Protection Legislation (系统构筑个人信息保护立法的基本权利模式). Law Science (法学), 2016, Vol. 4, pp. 67-80.

SVANTESSON, Dan Jerker B, A "Layered Approach" to the Extraterritoriality of Data Privacy Laws. International Data Privacy Law, 2013, Vol. 3, pp. 278-286.

SVANTESSON, Dan Jerker B, Extraterritoriality in Data Privacy Law. Ex Tuto Publishing, Denmark, 2013.

SVANTESSON, Dan Jerker B, Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation. International Data Privacy Law, 2015, Vol. 5, pp. 226-234.

SVANTESSON, Dan Jerker B, The Extraterritoriality of EU Data Privacy Law - its Theoretical Justification and Its Practical Effect on US Businesses. Stanford Journal of International Law, 2014, Vol. 50, p. 53-85.

TAYLOR, M. S. C., et al. Permissions and prohibitions in data protection jurisdiction. Brussels privacy hub working paper 2016, Vol. 2, p. 17-23.

TAYLOR, Mistale, The EU's Human Rights Obligations in Relation to its Data Protection Laws with Extraterritorial Effect. International Data Privacy Law, 2015, Vol. 5, No. 4, pp. 246-256.

TOWFIGH, Emanuel V.; ULRICH, Jacob, Art. 4, in: SYDOW, Gernot, EU GDPR (Europäische Datenschutzgrundverordnung). Nomos, 2nd Edition 2018, p. 6, 226.

TU, Zhenyu (屠振宇), Research on the Right to Privacy in the Constitution (宪法隐私权研究). Law Press (法律出版社), 2008, pp. 176-187.

TURBAN, Efraim; WHITESIDE, Judy; KING, David; OUTLAND, Jon, Introduction to Electronic Commerce and Social Commerce. Springer, 2017.

UECKER, Philip, Extraterritorial Regulatory Jurisdiction in Data Protection Law (Extraterritoriale Regelungshoheit im Datenschutzrecht). Nomos, Baden-Baden, 2017.

VERMEULEN, Gert; LIEVENS, Eva (Hg.), Reconciling the (Extra)territorial Reach of the GDPR with Public International Law. Data Protection and Privacy Under Pressure, Transatlantic Tensions, EU Surveillance and Big Data, 2017, p. 96.

VOIGT, Paul, Requirements for Third Country Transfers-Unresolved Issues (Anforderungen an Drittlandtransfers-ungeklärte Fragen). Computer und Recht, 2020, Vol. 36, No. 5, p. 319.

VOIGT, Paul, Art. 49, in: SPINDLER, Gerald; SCHUSTER, Fabian, Electronic Media Law (Recht der elektronischen Medien). C.H.Beck, 4th Edition 2019, p. 4, 18.

WANG, Chunhui (王春晖), Comparison of GDPR Personal Data Rights and Personal Information Rights in the Cybersecurity Law (GDPR 个人数据权与《网络安全法》个人信息权之比较). Cyberspace Strategy Forum (网络空间战略论坛), 2018, Vol. 7, pp. 41-43.

WANG, Xiuzhe (王秀哲), Research on the Constitutional Protection of the Right of Privacy (我国隐私权的宪法保护研究). Law Press (法律出版社), 2011, pp. 38-46.

WANG, Zhizheng, Systematic Government Access to Private-Sector Data in China. International Data Privacy Law, 2012, Vol. 2, No. 4, pp. 220-229.

WILL, Michael, Art. 42, in: EHMANN, Eugen; SELMAYR, Martin, General Data Protection Regulation (Datenschutz-Grundverordnung). C.H.BECK, 2nd Edition 2018, p. 35.

WOLFF, Heinrich Amadeus, VI. International Data Traffic with Countries Outside the Union (Internationaler Datenverkehr mit Staaten außerhalb der Union), in: SCHANTZ, Peter; WOLFF, Heinrich Amadeus, The New Data Protection Law (Das neu Datenschutzrecht). C.H.BECK, 1st Edition 2017, p. 1285.

XIONG, Xulong (熊谓龙), Right, or legal interest? -Re-discussion on the Nature of General Personality Rights (权利，抑或法益？- 一般人格权本质的再讨论). Journal of Comparative Law (比较法研究), 2005, No. 2, pp. 51-57.

YAO, Yuerong (姚岳绒), On the Justification of the Right of Information Self-determination as a Basic Right in China (论信息自决权作为一项基本权利在我国的证成). Political Science and Law (政治与法律), 2012, No. 4, pp. 72-83.

YE, Mingyi (叶名怡), On the Basic Category of Personal Information Right (论个人信息权的基本范畴). Tsinghua University Law Journal (清华法学), 2018, Vol. 5, pp. 143-158.

YU, Lu; AHL, Bjorn, China's Evolving Data Protection Law and the Financial Credit Information Systen: Court Practice and Suggestions for Legislative Reform. Hong Kong Law Journal, 2021, Vol. 51, p. 6, 19, 287.

ZANFIR-FORTUNE, Gabriela, Art. 82, in: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher, The EU Data Protection Regulation (GDPR): A Commentary. Oxford University Press, Oxford, 1st Edition 2020, p. 1175.

ZERDICK, Thomas, Art. 44, in: EHMANN, Eugen; SELMAYR, Martin, General Data Protection Regulation (Datenschutz-Grundverordnung). C.H.BECK, 2nd Edition 2018, p. 7.

ZERDICK, Thomas, Art. 47, in: EHMANN, Eugen; SELMAYR, Martin, General Data Protection Regulation (Datenschutz-Grundverordnung). C.H.BECK, 2nd Edition 2018,

p. 8.

ZHANG, Xiang (张翔), The Defensive Function of Fundamental Rights (论基本权利的防御权功能). Jurist Review (法学家), 2005, No. 2, pp. 65-72.

ZHANG, Xinbao (张新宝), Research on Personal Information Protection Provisions in "General Provisions of Civil Law" (《民法总则》个人信息保护条文研究). Peking University Law Journal (中外法学), 2019, Vol. 31, No. 1, pp. 54-75.

ZHAO, Hong (赵宏), The Status Quo of the Protection of Information Self-Determination in my Country and the Prospect of Its Legislation (信息自决权在我国的保护现状及其立法趋势前瞻). China Law Review (中国法律评论), 2017, No. 1, pp. 147-161.

ZHOU, Hanhua (周汉华), Personal Information Protection Law (Scholar Draft) (个人信息保护法（专家建议稿）及立法研究报告). Law Press (法律出版社), 2006.

ZHU, Xuanye (朱宣烨), Research on the Path of Civil Protection of Personal Information in the New Era - From the perspective of the distribution of responsibilities in the presence of third-party information processors (新时代个人信息民事保护路径研究-以存在第三方信息处理者情况下的责任分配为视角). Legal Science Magazine (法学杂志), 2018, Vol. 39, No. 11, p.8, 133-140.

II. Positions, Opinions and Guidelines of data protection authorities

Art. 29 Working Party, Adequacy Referential (updated), adopted on 28 November 2017 and endorsed by the EDPB on 25 May 2018.

Art. 29 Working Party, Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles", 16 May 2000.

Art. 29 Working Party, Opinion 8/2010 on Applicable Law, 16 December 2010.

Art. 29 Working Party, Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, 11 April 2018.

Art. 29 Working Party, Update of Opinion 8/2010 on Applicable Law in Light of the CJEU Judgement in Google Spain, 16 December 2015.

Art. 29 Working Party, Working Document 01/2016 on the Justification of Interferences with the Fundamental Rights to Privacy and Data Protection Through Surveillance Measures when Transferring Personal Data (European Essential Guarantees), 13 April 2016.

Art. 29 Working Party, Working Document on a Common Interpretation of Art. 26 (1) of Directive 95/46/EC of 24 October 1995, adopted on 25 November 2005.

Consumer Protection Association of Shanxi, "Leakage of Personal Information Mediated by the Consumer Protection Association", 7 May 2019.

Düsseldorfer Kreis, Guidance from the Düsseldorfer Kreis on the Legal Assessment of Case Groups for International Commissioned Data Processing (Handreichung des Düsseldorfer Kreises zur rechtlichen Bewertung von Fallgruppen zur internationalen Auftragsdatenverarbeitung), 28.03.2007.

EDPB, Frequently Asked Questions on the Judgement of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner *v* Facebook Ireland Ltd and Maximillian Schrems, 23 July 2020.

EDPB, Guidelines 05/2020 on Consent under Regulation 2016/679, 4 May 2020.

EDPB, Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679, 25 May 2018.

EDPB, Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3), version 2.1, 07 January 2020.

EDPB, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, Version 2.0, 18 June 2021.

EDPS, Opinion of the European Data Protection Supervisor of 7 March 2012 on the data protection reform package, 7 March 2012.

EDPS, The Transfer of Personal Data to Third Countries and International Organizations by EU Institutions and Bodies, 14 July 2014.

III. Case Law

CJEU, C-101/01, Lindqvist, 06.11.2003.

CJEU, Joined Cases C-92/09 and C-93/09, Schecke and Eifert, 09.11.2010.

CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland, 08.04.2014.

CJEU, C-131/12, Google Spain, 13.05.2014.

CJEU, C-230/14, Weltimmo, 01.10.2015.

CJEU, Case C-201/14, Bara and Others, 01.10.2015.

CJEU, Case C-362/14, Schrems I, 06.10.2015.

CJEU, Case C-203/15, Tele2, 21.12.2016.

CJEU, Case C-311/18, Schrems II, 16.07.2020.

Court of Appeal Berlin (KG Berlin), 20 SCH 13/04, 18.05.2006.

Federal Constitutional Court of Germany (BVerfG), Case 1 BvR 269/83, 15.12.1983.

Guangdong Higher People's Court, Yu Bingwen Financial Administration Case, Second-instance Administrative Ruling, 19. 05.2017.

Kolmar Group AG *vs.* Jiangsu Textile Group, (2016) 苏 01 协外认 3 号, Intermediate People's Court of Nanjing, 09.12.2016.

Liu Li *vs.* Tao Li, Dong Wu, (2015) 鄂武汉中民商外初字第 00026 号, Intermediate People's Court of Wuhan, 30.06.2017.

Ma *vs.* Symantec, (2011) 沪高民三（知）终字第 88 号, the Superior People's Court of Shanghai, 08.04.2012.

Sascha Rudolf Seehaus, (2012) 鄂武汉中民商外初字第 00016 号, Intermediate People's Court of Wuhan, 26.11.2013.

IV. Internet Source

ARMINGAUD, Claude-Etienne, EU Data Protection: in a Post-Privacy Shield, Sectoral Code of Conduct Could Lead the Way to Safeguard Data Transfers Outside the EU/EEA, 17 July 2020, available at: https://www.klgates.com/eu-data-protection-in-a-post-privacy-shield-sectorial-code-of-conduct-could-lead-the-way-to-safeguard-data-transfers-outside-the-eueea-07-17-2020. Last visited on 14.10.2023.

AHMAD, Imran, Extraterritorial Scope of GDPR: do Canadian businesses Need to Comply? available at https://www.millerthomson.com/en/blog/mt-cybersecurity-blog/extraterritorial-scope-gdpr-canadian-businesses-need-comply/. Last visited on 01.06.2020.

Background Paper of the Bundeskartellamt's Working Group on Competition Law, Digital Economy - Internet Platforms Between Competition Law, Privacy and Consumer Protection (Hintergrundpapier des Arbeitskreises Kartellrecht des Bundeskartellamts, Digitale Ökonomie – Internetplattformen zwischen Wettbewerbsrecht, Privatsphäre und Verbraucherschutz), https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Diskussions_Hintergrundpapier/AK_Kartellrecht_2015_Digitale Oekonomie. html, p. 8-9. Last visited on 16.02.2020.

Cross-border E-Commerce Shopper Survey 2019 (public version), International Post Corporation, available at https://www.ipc.be/services/markets-and-regulations/cross-border-shopper-survey. Last visited on 09.02.2020.

GRUGGENBERGER, Nikolas; DEMARY, Vera; RUSCHE, Christian Rusche, Data Sharing im E-Commerce-Rechtliche und ökonomische Grundlagen, 9. October 2019, available at: https://www.iwkoeln.de/fileadmin/user_upload/Studien/Gutachten/PDF/2019/Gutachten_Data_Sharing_Final.pdf. Last visited on 13.02.2020.

http://history.mofcom.gov.cn/?newchina= 跨 境 电 商 蓬 勃 兴 起 . Last visited on

08.02.2020.

http://www.crossborder-ecommerce.com/international-expansion/. Last visited on 11.02.2020.

https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc. Last visited on 20.09.2020.

https://www.marketplacepulse.com/about. Last visited on 17.03.2020.

https://www.marketplacepulse.com/articles/china-share-of-amazon-marketplace-is-likely-as-much-as-25-percent. Last visited on 17.03.2020.

https://www.marketplacepulse.com/articles/one-million-new-sellers-on-amazon. Last visited on 17.03.

https://www.marketplacepulse.com/marketplaces-year-in-review-2018#wish. Last visited on 17.05. 2020.2020.

International Law Commission, Report on the Work of the Fifty-eighth Session (2006), Available at http://legal.un.org/ilc/reports/2006/. Last visited on 24.02.2019.

International Law Commission, Report on the Work of the Fifty-eighth Session (2006), Available at http://legal.un.org/ilc/reports/2006/. Last visited on 15.07.2020.

MANN, Friedrich Alexander, The Doctrine of Jurisdiction in International Law (Volume 111). Collected Courses of the Hague Academy of International Law. Available at: http://dx.doi.org/10.1163/1875-8096_pplrdc_ej.9789028614826.001_162.2. Last visited on 16.06.2020.

MICHAELS, Ralf, Recognition and Enforcement of Foreign Judgements. Max Planck Encyclopedias of International Law. Available at: athttps://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1848. Last visited on 22.08.2020.

OECD, An Introduction to Online Platforms and Their Role in the Digital Transformation, https://www.oecd.org/innovation/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation-53e5f593-en.htm. Last visited on 15.02.2020.

OECD, Unpacking E-Commerce: Business Models, Trends and Policies, OECD Publishing, Paris, 2019, available at https://doi.org/10.1787/23561431-en. Last visited on 15.02.2020.

Publishing, Paris, 2019, available at https://doi.org/10.1787/53e5f593-en, p. 68. Last visited on 16.02.2020.

SENTENCE, Rebecca, Websites are Blocking Visitors From the EU? 31 May 2018, available at: https://econsultancy.com/gdpr-which-websites-are-blocking-visitors-from-the-eu-2/. Last visited on 23.11.2020.

YI, Meijin, Comment to the Information Security Technology - Personal Information Security Specification, available under https://www.tc260.org.cn/front/postDetail.html?id=20180201200746, last visited on 05.03.2021.