TALLINN UNIVERSITY OF TECHNOLOGY

School of Business and Governance

Department of Law

Sodiq Saheed

Extraterritorial Impact of the General Data Protection Regulation (GDPR), a case study of The Chinese Adoption Model

Bachelor's thesis

Programme Law, specialization EU and International Law

Supervisor: Dr. Maria Claudia Solarte-Vasquez

Tallinn 2021

I declare that I have compiled the paper independently

and all works, important standpoints and data by other authors

have been properly referenced and the same paper

has not previously been presented for grading.

The document length is 8,885 words from the introduction to the end of the conclusion.

Sodiq Saheed……

(signature, 13 May 2021)

Student code: 183960HAJB

Student email address: saintdolap@yahoo.com

Supervisor: Maria Claudia Solarte-Vasquez, PhD:

The paper conforms to requirements in force.

…….

(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

……..

(name, signature, date)

TABLE OF CONTENT

ABSTRACT

The European Union (EU) digital rights strategy has advanced remarkably in the consolidation of the data protection rules and standards. The EU has set global standards and pioneered regulatory tools for General Data Protection Regulation adoption. The process compares to that of major global powers or business partners, or active players in digital trade, in establishing similar standards of protection. Controllers located outside of the EU whose data processing activities correlate to such business interest are currently subject to the laws set out in the General Data Protection Regulation. This study will focus on the restrictive impact of fundamental problem with development of privacy protection, as Chinese companies are being subjected to less restrictive data protection rules than EU-based companies because China lacks an extensive data protection structure. GDPR protects all data subjects regardless of their nationalities in the EU, and control cross-border data transfers towards non-EU nations. Over the years, China's approach towards stronger data protection is commendable.

This thesis will explore the Chinese adoption model of GDPR by data controllers and processors in China regarding uniform compliance with CCL and GDPR. It will stress on the evidence showing that big Chinese organizations generally found compliance with GDPR achievable, many companies already putting measures in place to be complaint with the regulation. However, research shows that compliance with GDPR posed adjustments investments costs. The document also proposes high-minded training models for controllers in line with CCL and GDPR standards.

Keywords: General Data Protection Regulation (GDPR), Extraterritorial reach of EU Regulations, China, European Union (EU), Extraterritorial GDPR Adoption

INTRODUCTION

The EU General Data Protection Regulation (GDPR), replaced the Data Protection Directive 95/46/EC on May 25th, 2018. The new regulation is considered a wide-ranging wedge of legislation with universal reach.[1]As the regulation took effect, [2]all companies with the responsibilities of processing personal data of EU citizen must comply, even if they are not based in the EU. [3]Multinational Corp of Chinese subsidiaries with headquarter in the EU are also affected because they process EU personal data. [4]According to Snowden's revelation of mass surveillance, which shows the weak exterritorial protection in the recent EU-US data transfers. The research focusses on China due to the rise in economy and the fast globalization of China's IT industry, an increasing number of EU citizens' personal data are collected and processed on Chinese territory.

The attention of both sides is drawn as [5]China is EU's second largest trade partner, while EU is China 's largest trade partner. In view of this, there is a huge amount of cross-border data transfers considering their steadily growing political, economic, and societal connections. Therefore, it is important to understand whether the Chinese Cybersecurity Law is a suitable adoption model?

Thesis paper also proposes high-minded training models of controllers and processors through binding written agreements that provide sufficient guarantees that the processing will meet the requirements of the GDPR and ensure the rights of the data subject[6]. This research emphasizes on how GDPR poses burden of compliance for organizations with EU clients in China[7]and adoption model of GDPR by

[1] Michael Tan. (2018), Government guidance for Chinese businesses on GDPR compliance
[2] Michael Nadeau. (2020), General Data Protection Regulation (GDPR): What you need to know to stay compliant
[3] Michael Tan. (2018), Supra notra 1
[4] Ibid.,3
[5] European Commission https://ec.europa.eu/trade/policy/countries-and-regions/countries/china/
[6] Jared Nelson, Shi Yuhang, (2018), The GDPR's Effects In China: Comparison With Local Rules And Considerations For Implementation
[7] KPMG. (2018), Extraterritorial scope of GDPR. The Impact of the GDPR on Organizations in Asia.

controllers regarding compliance with GDPR standards. How can the Chinese adoption model integrate the impact of EU Extraterritoriality on data controllers in China?. Data controllers around the world seems wary of incurred risk of non-compliance with the Regulation; [8]regardless if they are of the Internet giants, a non-EU company that offers services to EU consumers, companies with cookies that track EU consumers. The author will compare the adoption model of GDPR and CCL by systematically analysing their differences and identify the impact of the Extraterritoriality. From 24th of May 2018, the violation of EU General Data Protection Regulation will be punishable by a sanction of up 100 million or 4% of the yearly worldwide turnover in case of an enterprise. The Data Protection Authorities (DPAs) are charged with the responsibility of imposing these sanctions and will be adequately equipped with a wide range of tasks and authority on top. [9]The GDPR proposes a range of new personal rights designed to protect consumers whose personal information is collected, processed, and saved by companies and other entities.[10]Most in particular, the draft regulation would create a consumer's "right to be forgotten", prompting organizations that collect data to delete any data relating to a data subject. The European Data Protection Board's majority binding decisions can force any Member States' DPA to change, adopt or withdraw a certain measure. The harmonized and synchronized applicable data protection law for the European Union replaces almost all the existing Member States' provisions. GDPR facilitates data flows within the EU, protecting the data subjects through established law and implementation mechanism. This includes the right to information, objection, explicit content, data erasure (the right to be forgotten), data portability, data rectification and remedy, etc. However, there have been uncertainties over the protection of the fundamental right in the state of affairs of exterritorial applications of the corresponding GDPR rules. The gathering of data requires accountability and transparency, the combined effort is essential for the completion of a specific aim.

[8] Azzi, A. (2018). The challenges faced by the extraterritorial scope of the general data protection regulation. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 9(2),* 126-137.

[9] Victor, J. M. (2013). The EU General Data Protection Regulation: Toward Property Regime for Protecting Data Privacy. Yale Law Journal, 123(2), pg 513

[10] Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, COM (2012) 11 final (Jan. 25, 2012), http://www.europarl.europa.eu/registre/docs _autres institutions/commission europeenne/com/2012/ooll/COM COM%282012%290011 EN.pdf [hereinafter Draft Data Protection Regulation]. The draft Regulation seems to be primarily designed to regulate data processing by private entities. While some agencies of EU member-states may also be bound by the Regulation, the majority would fall outside its purview. See id. art. 2(2) (listing, inter alia, "Union institutions, bodies, offices and agencies" and authorities devoted to the "prevention, investigation, detection or prosecution of criminal offences" as entities that are not bound by the Regulation).

The research paper has three chapters, the first is dedicated to the historical antecedents of GDPR and Chinese rules to understand the integration of the Chinese adoption model of data protection. The section also to discusses the relationship between the two legislations and Extraterritoriality impact. The second examines the General Provisions and Principles of General Data Protection Regulation and challenges of Right To Be Forgotten in China for data controllers in adoption model. The final chapter proposes amendments to the CCL to match the GDPR Standards, even though there are similarities in both Regulations, an identical legislation uniformity will ensure adequate compliance. Additionally, it is recommended to employ intellectual data controllers with legal background who can decipher what data protection entails to ensure high quality standards.

The internet is compared to a space where no conventional border exists[11].Extraterritoriality is defined the competence of a State to draft, apply and enforce rules of conduct regarding property, persons, or events beyond its territory[12]. [13]The GDPR profess an extensive extraterritorial jurisdiction to secure all data subjects on the EU territory regardless of their nationalities when their personal data are transferred to countries outside the EU. In 2018, the GDPR came into force after a several phases of law-making decision. The DIR95 is no longer obtainable due to present day digital environment, GDPR aim to improve the level of harmonization and personal data protection across the EU. [14]The GDPR replaced the 1995 Directive and a Directive, the [15]Police and Criminal Justice Data Protection Directive, the 2008 Data Protection Framework Decision. [16]In 2009, the process started through a relevant public consultation launched by the Commission, culminated in early 2012,[17]upon proposals published by the Commission which required at least three years to pass through the Council's and Parliament's scrutiny. The fine for non-compliance with the regulation has been harmonized and increased significantly. In case of minor violation, organizations can be sanctioned up to 10 million euros.

[11] Alexander Garrelfs. GDPR Top Ten #3: Extraterritorial applicability of the GDPR
[12] Menno T Kamminga, (2020), Oxford Public International Law
[13] Zhao, B., & Chen, W. (2019). Data protection as fundamental right: The european general data protection regulation and its exterritorial application in china. US-China Law Review, 16(3), pg 97
[14] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, pp. 31–50.
[15] On The Right To Be Forgotten see: Paul De Hert. Vagelis P. (2012). The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. Computer Law & Security Review 28(2): pg 130-142
[16] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350/60, 30.12.2008
[17] Ibid.,16

However, a warning could be given for first offences and fines of up 4% of worldwide revenue can be imposed or 20million euros for more serious violations.

As a major inclusion to China's general framework, the Personal Information Security (Specifications) entered effect in May 2020[18]. Companies in compliant with Chinese rules must also adhere to GDPR,[19]the specifications come with underlying scopes and content with the EU rules. [20]The lack of unified legislation on data protection in China makes comprehension and enforcement more difficult. [21]The business activities of companies in China that process EU resident's data are directly affected and risk violating the law in the case of non-compliance.

The territoriality principle based solely on jurisdiction has become less evident, Article 3(2)a of the GDPR brings non-EU data controllers and processors under the GDPR when they process EU citizen's data. Further, Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) lay out specifically that everyone has the fundamental right to the protection of personal data regarding him or her. Freedom from right to privacy and creation of positive right appear to be a leading characteristics of the EU legal order, which has promoted data protection to the peak status of fundamental right in EU law. [22]According to the EU law context, other than constitutional rights and human rights, the term "fundamental rights" is commonly referred to.

Specifically,[23] it provides security for citizens in managing and controlling their personal data[24]. [25]Trust concerns can slow down the advancement of the innovative use and adoption of new technologies, also new business opportunities may be hindered if proper data protection practices are not implemented. [26]Due to the significant technological advancement, companies increasingly tend to use data for numerous purposes such marketing and personalized services. [27]Since companies can easily collect and

[18] Jared Nelson, Shi Yuhang, (2018), supra notra 6
[19] Ibid.,18
[20] Anja Geller, How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective, *GRUR International*, Volume 69, Issue 12, pg 1191
[21] Zhao, B., & Chen, W. (2019). Supra notra 13,97
[22] Ibid., 21
[23] Alessandro Mantelero (2013), The EU Proposal for a General Data Protection Regulation, and the roots of the 'right to be forgotten', *Computer Law & Security Review*, Volume 29, Issue 3, Pg 229-235
[24] Van Ooijen, I., Vrabec, H.U. (2018), Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *J Consum Policy* **42,** pg 91
[25] Viviane Reding (2011), The upcoming data protection reform for the European Union, International Data Privacy Law, Volume 1, Issue 1, Pg 3
[26] Ibid.,25
[27] Ibid.,25

process data, increased challenges for personal data protection have emerged. [28]Solicitous effort by China has enhanced data protection by propagating fresh laws and updating old laws to the standard that meets challenges of the information economy, which is considered as the driving force of China's future economic growth. [29] There have been doubts regarding the protection of the fundamental right in the context of Extraterritorial implication of related GDPR rules. [30]Data controllers and processors in China automatically fall under the scope of GDPR the moment they process EU resident's personal data. Apparently, business activities will be directly affected and a high-risk potential law violation in case they fail to follow GDPR's data protection requirements.

This regards the strict data localization and internet censorship rules, which limit information flows, rendering extraterritoriality less important. [31]Prior to CCL, [32]an in-depth analysis of data protection regime of China was done by The Directorate-General for Internal Policies. According to this report, there is no traces of proper data protection found in a multitude of sector-specific legal instruments[33]. There was no specific policy before China's Cybersecurity with a concentration on data protection principles, data transfers, individual rights, and enforcement mechanism[34]. Cloud service enhanced data transfer between the EU and China in an online setting.

The[35]traditional legal research method is adopted in the research due to the differences between the legal framework of jurisdictions as importing rules and solutions from abroad may not work because of differences in extraterritoriality[36]. Accordingly, the analysis collected from various sources will be employed to compare the territories of study to investigate areas of recommendations. An initial approach to the research entails sourcing for academic articles giving a general overview on the data protection and Extraterritorial application in China. This search was conducted by skimming through the literature on enforcement of GDPR by data controllers and processors in China in the catalogue of

[28] Bo Zhao, G.P. (Jeanne) Mifsud Bonnici 2016, Protecting EU citizens' personal data in China: a reality or fantasy?, International Journal of Law and Information Technology, Volume 24, Issue 2, Pages 128-150
[29] Zhao, B., & Chen, W. (2019). Supra notra 13, 98
[30] Territorial scope of the GDPR (Article 3)
[31] Fan Yang, Jian Xu. (2018). Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law. Asia and the Pacific Policy Studies, Vol:5 Issue :3 pg 538
[32] Paul De Hert, Vagelis P. (2015), The Data Protection Regime in China. In-Depth Analysis
Brussels Privacy Hub Working Paper, Volume 1, Number 4
[33] Prud'homme D., Zhang T. (2019) Statutory IP Laws. In: China's Intellectual Property Regime for Innovation. Springer, Cham. https://doi.org/10.1007/978-3-030-10404-7_2
[34] OECD (2000-09-21), "Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks", OECD Digital Economy Papers, No. 66, OECD Publishing, Paris.
[35] Myths on the extraterritorial scope of the GDPR
[36] Van Hoecke, M. (2015). Methodology of Comparative Legal Research. Law and Method. pg 8

Tallinn University of Technology, with access to the most relevant articles from different online databases. The data for this study were retrieved from Google Scholar, the database was scanned for relevant articles. The term “Extraterritorial impact “was used as search topic in the first stage. The academic work of Alessandro M, Reding V, Zhao B, and Chen W, business between EU and China. In addition, more compendious and updated literature regarding these issues has been sought from the ResearchGate, Hein Online and ScienceDirect databases.

I hereby express my sincere gratitude to my supervisor in person of DR. Solarte-Vasquez for the unrelented support and legal guidance both in class and during personal consultations. I would also like to thank my parents, Mr & Mrs Saheed, for their support throughout my educational career.

1. THE LEGAL FRAMEWORK AND LANDSCAPE OF GDPR

1.1 Data Protection

The Extraterritorial Application of data protection law presently effectuate similar obligation as would an international legal framework[37], [38]it extends protection by law to the processing of personal data regardless of their location. [39]Digital Technologies benefits entail unknown privacy risks that arose due to reality of collecting, processing, storing, and using of data. [40]The advent of automated data systems created a significant increase in the sum of data and the prospect of processing it. [41]Transborder data flow affairs are apparently the most influential that confronts the Directive. [42]The word data is the plural of datum, neuter past particle of the Latin word dare "to give", hence "something given". [43]Origin

[37] Christopher Kuner. (2015). The European Union and the Search for an International Data Protection Framework. Groningen Journal of International Law, Vol:2 N0 2, pg 64
[38] Ibid., 37
[39] Burri, M., & Schär, R. (2016). The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. *Journal of Information Policy*, *6*, pg480
[40] Michael D. Birnhack. (2008). The EU Data Protection Directive: An engine of a global regime, Computer Law & Security Review, Volume 24, Issue 6, pg 551
[41] Yves Poullet. (2006). EU data protection policy. The Directive 95/46/EC: Ten years after, Computer Law & Security Review, Volume 22, Issue 3, pg 211
[42] https://www.definitions.net/definition/data
[43] Ibid.,42

of data as concept in data processing consist of words, images, information, and numbers. [44]Data protection in some countries is fused with the concept of privacy, with the interpretation as managing personal information. The increase in data processing and collection evoked debate on information privacy and led out the need for personal data protection[45]. [46]The right to data protection can find its origin partially in the data protection rules of countries in the Northern Europe,[47] it arose in several nations in the 1970s, and the Council of Europe's Resolutions on data processing and the realization of fair Information (FIPs).

The personal data protection directly applies to EU member states, [48]to end the cumulative and simultaneous application of different domestic data protection laws. Subsequently, the law is extended outside the EU, [49]this is evident in the case of EU data protection law that applies to processing of data outside the EU. [50]Restrictions are placed on transborder data flows which ensures EU data protection standards are enforced in data processing of EU residents. Currently, [51]The citizens of European Union remarkably enjoy powerful protection of personal data within the EU. The protection of EU's data protection legal framework is considered weak when cross-border transfer of data and laws of jurisdiction concerns are at stake. [52] The key attention of Europe focusses on protection of EU citizen's personal data transferred to the United State, while data transferred to other big market actors such has China were largely neglected. [53]The Regulation takes the extra-ordinary step by introducing a property regime in personal data, under which the personal property entitlement belongs to the data subject and alienable partially. [54] The EU's proposal includes three elements to a property-based conception: the data, regardless if its transferred carries a burden that runs with it and attach third parties; consumers are entitled to their personal data and consumers are protected through remedies grounded in property

[44] Simon Davies. (1996). "Big Brother: Britain's web of surveillance and the new technological order", Pan, London, p. 23
[45] Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies, Computer Law & Security Review, Vol:34, Issue 1, pg 134
[46] Zhao, B., & Chen, W. (2019). Supra notra 13,100
[47] Bart van der Sloot. (2014). Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation, International Data Privacy Law, Vol: 4, pg 307
[48] Viviane Reding. (2012). The European data protection framework for the twenty-first century, *International Data Privacy Law*, Volume 2, Issue 3, pg 121
[49] Christopher Kuner. (2015). Sopra notra 42, 64
[50] Ibid., 49
[51] Bo Zhao, G.P. (Jeanne) Mifsud Bonnici (2016), supra notra 28, pg 128–150
[52] Ibid., 51
[53] Victor (2013). Supra notra 20, 515
[54] Ibid., 53

rules. [55]Responsibilities are imposed on data controllers by the Directive and cede some rights to the data subject. [56]The Directive was apparently drafted with a keen interest regarding the way third countries would respond. [57]The system of checks and balances aim to protect individuals whenever their personal data is processed, which is viewed as modern right.[58]Not only did Article 8 of the EU Charter of Fundamental Rights affirmed the right to personal data protection, however, justifies the core values associated with this right.[59]It states that provision of data processing must be fair and for designated purposes. [60]Compliance regarding this right is crucial and contingent upon control by an independent authority.

The adoption of the Lisbon Treaty is a turning point in the evolution of data protection law[61],[62]the territorial scope of the Regulation now has comprehensive rules applies to controllers and processors from third countries that offer services to data subjects residing in EU or monitor their activities. [63]An efficacious universal legal framework for data protection requires transparency regarding rules of applicable law.[64]The organization responsible for drafting transnational data protection rules are hesitant to deal with topic of applicable law because of its intricacy and the fear of fortuitous consequences. The GDPR requires data controller to process personal information fairly and in a transparent manner. Therefore, Art 6 and 9 the GDPR describe the criteria to be meant in order for data processing to be lawful. Consent is a lawful basis for data process and the party processing data subject's data may choose different options foreseen in the GDPR Article 6. If the data controller is unable to translate the basis for processing, it will be unable to proceed.

[65]So far, the only international data protection instrument is EU Data Protection Directive (now GDPR) to contain rules on applicable law. [66]EU proceeded to further global protection of personal data by

[55] Michael D. Birnhack. (2008). Supra notra 46, 513
[56] Ibid., 55
[57] Advocate General Sharpston described the case as involving two separate rights: the "classic" right to the protection of privacy and a more "modern" right, the right to data protection. See CJEU, Joined cases C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston, 17 June 2010, para. 71.
[58] Hustinx, P. (2013). EDPS Speeches & Articles, EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation.
[59] Ibid.,58
[60] Ibid.,
[61] Handbook on European Data Protection Law (2018) edition, pg 28
[62] Ibid., 61
[63] Kuner, C. (2013) Transborder Data Flows and Data Privacy Law, Oxford, Oxford University Press, pg 125–129
[64] Christopher Kuner. (2015). Supra notra 42, 64
[65] With regard to the failure of the Council of Europe Convention 108 to include clear rules on applicable law, see Bygrave, L., (2014) Data Privacy Law: An International Perspective, Oxford University Press, Oxford, pg 2057-2058
[66] Christopher Kuner. (2015). Supra notra 42, 69

adopting its own standards model extraterritorially, instead of deliberating on a new set of standards on an international level. [67]Jurisdiction as a law operates on the principle of permissions. [68]The EU is permitted to broaden the geographic scope of EU law on the authority of passive personality. [69]The territorial scope of a fundamental right enshrined in the Article 8 accompanies the scope of the EU's adroitness and the application of EU law.

In 2014, China had to move towards steps to integrate with protection of personal data, however, we all agree that the approach was quite sparse[70].[71]Despite the increased engrossment in building a stronger data protection regime by the Chinese government, it is mostly perceived as being ineffective and difficult to comprehend. The framework of GDPR can be used to organize Chinese law to make it more comprehensible[72], which will be discussed in the chapter.

To conclude, the GDPR was set out to provide standardized data protection law, not only against data controllers within the EU, however, the territorial scope extends outside the EU as Extraterritorial application. The effect influences not only the technical-know-how in handling sensitive data, however, having strong knowledge of foreign laws which guide and protect data subject.

1.2. Overview of GDPR and CCL

[73]It has been claimed that traditional Chinese culture is the main cause of the lack of privacy protection. China is experiencing a rapid progress of its data privacy framework[74], [75]the Cybersecurity Law took

[67] Ryngaert, C., & Taylor, M. (2020). The GDPR as Global Data Protection Regulation? *AJIL Unbound, 114*, pg 6
[68] Ibid., 67
[69] Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1 (Dec. 18, 2000)
[70] Graham Greenleaf, The influence of European data privacy standards outside Europe: implications for globalization of Convention 108, 2 INT'L DATA PRIV. L. 68, pg 72
[71] see Yang Feng, 'The Future of China's Personal Data Protection Law: Challenges and Prospects' (2019) 27 Asia Pac L Rev 62f, 68; Xiaodong Ding (丁晓东), 'The Dual Attributes of Personal Information and a Behaviouristic Regulation (个人信息的双重属性与行为主义规制)' (2020) 0(1) The Jurist (法学家) 64, 76;
[72] Anja Geller (2020), supra notra 17, 1191
[73] Emmanuel Pernot-Leplay (2020). Data Privacy Law in China: Comparison with the EU and U.S. Approaches. Pg 51
[74] Ibid., 73
[75] Eric W. Huang. (2018). China: An overview of China's New Cybersecurity Law

effect on June 1, 2017. [76]Prior to the adoption of the new law, China already had regulations that governs data and privacy protection.[77]However, the adoption shows China's commitment and attention towards data protection.[78]In a wider sense of term, CCL is not focused mainly on internet security, but also communication security, automation, information security and control system security. [79]Substantially, the impact of CCL on business are not restricted to those in information technology (IT) industry. [80]The GDPR strive to exceed expectation by meeting the challenges related to personal data protection by building up online privacy rights and boosting Europe's digital economy. It is important to keep in mind for purposes of understanding and applying EU data protection laws and the hostility is probably the reason European companies do not lead in information driven economy sectors such as, Electronic Commerce, Cloud Computing, Software as a Service (SaaS) and Social Networking. [81]To broaden the China's Cybersecurity Law, the Chinese government introduced the final version of a new national standard on personal data protection, which took effect on May 1, 2018. Cloud service enhanced data transfer between the EU and China in an online setting. GDPR to propose solutions for harmonization, to facilitate the ease of data transfer for smooth economic relation between EU and China, it is compulsory for data controllers and processors in Chinese territory to adhere with GDPR, if China's Cybersecurity Law is comparable to that of the GDPR standard, the gap will be minimal. However, there is a huge legal gap on many fronts. [82]The main challenge linked to the application of the GDPR is the companies' lack of awareness and understanding of the requirements that the GDPR obtrude through its laws.[83]The requirements enshrined in the GDPR have various pragmatic connotations for organizational practices and operations. The author compares differences between the two laws using a table as illustration.

[76] Ibid., 75
[77] Ibid.,
[78] Leo Zhao, Lulu Xia. (2018). China's Cybersecurity Law: An Introduction for Foreign Businesspeople
[79] Ibid., 78
[80] A. Mantelero. (2013). Supra notra 23, 230
[81] Yong Yan.S. (2018). The impact of the GDPR and China's data protection regime towards Chinese cloud service providers with regards to cross-border data transfers. Master's Thesis, Tilburg University, Tilburg Law School 2018, 9.
[82] Tikkinen-Piri C, Anna R, J Markkula. (2018). Supra notra 45, 135
[83] Ibid., 82

Table 1. Comparison between GDPR and Chinese Rules

Item	GDPR	Chinese Rules
Key Categories of Entities	Data Controller Data Processor Data Recipient	Network Operator Network Product/Service Provider Critical Information Infrastructure Operator Personal Information Controller Personal Information Processor
Age for Protection of Children	16 years old	14 years old
Right To Be Forgotten and Deletion Right	Data subjects have the fundamental right to acquire from the controller the erasure of personal information in several conditions, including where: (a) the personal data is no longer necessary in relation to the purposes for which it was collected or[84] otherwise processed; or (b) the data subject withdraws consent and there is no other ground for the processing.	Data subjects have the right to obtain from the controller the erasure of personal information in several conditions, including where: (a) controllers violate provisions of the laws and regulations in collecting or using personal information; or (b) controllers violate agreements with the data subject in collecting or using personal information.

Source: Jared Nelson and Shi Yuhang. (2018). China: The GDPR's Effects in China: Comparison with Local Rules and Considerations for Implementation.

As stated above, [85]the Chinese rules and GDPR share many similar attributes and specifications. Data subject under the Chinese rule cannot request for personal data to be erased unless data breach or violation has occurred. Unlike GDPR, the fundamental right of data subject seems quite limited. [86]There are common requirements, definitions, focusses and implementation time frame.[87]Full scale compliance under either set of legislations guarantees coverage of different scope of obligations in both jurisdictions, however, there are some significant differences and notable gaps. The author views that the Chinese government has made significant steps to be compliant with GDPR, hence the introduction

[84] Ibid.,
[85] Ibid.,
[86] Ibid.,
[87] Ibid.,

similar rules and standard in the adoption model. Making laws is quite different from enforcing it, China has a penchant of "looking away" in a situation where the law is violated. [88]The regulation will force organizations to restore order to their operations and ensure a little tidying up and it will deliver restrictions, it will also provide many benefits to business. The next chapter will discuss the extraterritorial application and the impact in China. It is believed that individuals' rights should be strengthened by ensuring a high level of protection and control over their personal data[89].

2.ANALYSIS OF EU EXTRATERRITORIAL METHODOLOGIES

2.1 EU Extraterritorial Impact in China

The lawful transfer of data to third country according to GDPR requires protection outside the jurisdiction of EU[90],[91]There must be adequate protection and decision which guarantees derogations under specific circumstances.[92]According to Article 58 of the GDPR, data protectors and controllers can be ordered to stop or suspend data processing, provide necessary information regarding data subject should the need arises. [93]Irrespective of the geographical location, the Extraterritorial jurisdiction avails the data subjects from the EU to lodge a proceeding against controllers to file for damages in accordance with Article 79. [94]The *Google Spain case* exhibit a propensity towards the expansion of the

[88] Jocelyn Krystlik. (2017), With GDPR, Preparation Is Everything, Computer Fraud & Security, Issue 6, pg 5
[89] Reding (2011). Supra notra 25. 4
[90] Zhao, B., & Chen, W. (2019). Supra notra 13, 100
[91] Ibid., 92
[92] Article 58 of the GDPR
[93] Zhao, B., & Chen, W. (2019). Supra notra 13, 100
[94] Case C-131/12 Google Spain and Google

territorial scope of application of EU data protection regulation so as to cover controllers with a primary establishment outside of the EU. The CJEU ruling in the *Google Spain case* marks the first time the provision of the Data Protection Directive determined its territorial scope in order to expand the application GDPR to a third-country controller that process EU resident's data from the US. [95]Data controllers are charged with meticulous responsibility of obliging with the GDPR to disclose to data subjects in a precise, clear and understandable manner. [96] The regulations protection personal information is quite dispersed in China; however, a more standardized legislation is imminent in the near future.

According to Article 35, companies were advised to consider carrying out a Data Protection Impact Assessment (DPIA). [97]DPIA is required when the processing of personal data[98] can result in a high risk to rights and freedoms of natural persons. The impact of GDPR to China indicates that trade flows in service is dramatically affected by privacy protection as compared to trade flows in good. When Chinese company offer services online to EU residents, GDPR applies regardless with a payment or not. [99]According to Article 1(1)(b), good and service entails offering of information and any service provided for payment at a distance through digital means and at the individual request for a recipient of services. [100]Chinese app platform service provider such as WeChat is widely used by EU residents, by default the company is a data controller or joint controller depending on the purpose and means of data processing. The extraterritorial scope is well discussed in the general provisions and principles of the Regulation, the next chapter elaborated on the controller's establishment.

2.2 General Provisions and Principles Of GDPR

The GDPR includes an expanded territorial scope for personal data processing operations according to Article 3[101], GDPR also applies to the processing of data by processors[102] or controllers that are not

[95] Anna Xue (2019). The impact of EU's GDPR in China. China Business Law Journal
[96] Ibid..96
[97] Article 35 of the GDPR
[98] Ibid.,98
[99] Article 1(1)(b) of the GDPR
[100] Zhao, B., & Chen, W. (2019). Supra notra 13, 107
[101] Christina Tikkinen-Piri, Anna Rohunen & Jouni Markkula (2018). Supra notra 45, Pages 135
[102] Ibid., 103

established in the EU, as long they offer goods and services to the data subject residing in the EU or monitor the data subjects' activities within the EU. [103]New definitions were introduced by GDPR to personal data intensive companies and their processing operations according to Article 4. The GDPR explains the provisions and principles for processing of data are majorly the same as those of DIR95, however, the GDPR introduced some additions: the transparency of data processing (Art. 5), accountability (Art. 5) and also data processing which doesn't require identification (Art. 11). [104]Prior any processing of personal data, a data subject must be informed and be aware of the purposes for which data will be processed. Also, information of the data controller's identity, recipients of his personal data and the period of data storage according to Article 13 and Article 14 of the GDPR. [105] The research conducted prior to the replacement of the Finnish Data Act by General Data Protection Regulation showed that 43% of the controllers were aware of the reform. 31% of the controllers said they were planning to act towards compliance as the willingness to take a step was quite low. The Regulation mandates a data controller to also provide the information about meaningful information about logic involved envisaged consequence and the existence of automated decision making, which includes profiling. [106] The Regulation's general provisions include new definition for pseudonymization, data protection policies, data breach and sensitive personal data types. Pseudonymization can be defined as the personal data processing in such way that the data shall not be designated to a specific data subject without additional information; such additional information is separated and subject to organizational and technical evaluation to ensure non-attribution.

The *Google vs Spain case* shed more light on extraterritoriality, the Court of Justice of the European Union (CJEU) decided that the activity of a search engine should be classified as 'processing of personal data' when the information contains personal data,[107]and explained that the operator of the search engine must be regarded as the 'controller' in respect of that processing.[108]Some certain situations warrants a search engine operator to delist specific results displayed following a search made

[103] Ibid.,
[104] Van Ooijen, I., Vrabec, H.U. (2018). Supra notra 24, **pg** 92
[105] Tomi Mikkonen (2014). Perceptions of controllers on EU data protection reform: A Finnish perspective. Computer Law and Security Review Vol. 30 .Issue 2. pg 190-195
[106] Christina, Rohunen, & Markkula (2018)., sopra nota 45, 138-139
[107] Dan Jerker B Svantesson (2015), Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, *International Data Privacy Law*, Volume 5, Issue 4, pg 226–234
[108] Ibid.,109

on the basis of a person's name[109]. [110]Cross-border data transfers to China can occur in unpredicted ways, drawing up greater data protection concerns at global level. [111]For instance, it is reported that Facebook has data sharing partnerships with not less than four Chinese electronic economic since 2010, delivering wide classified access of user data to Huawei, Lenovo, TCL, and Oppo without user's consent. [112]This data sharing avails the Chinese partners to recover detailed information on both device users and their close associates, including education history, political leanings, work, and relationship status. Such data sharing extends to manufacturers which includes Amazon, Blackberry, Apple, and Samsung[113]. [114]Human brain can easily forget information, how web can recollect nearly everything, data subject must be critical and wary to take extraordinary steps in other to forget. [115]Contrary to human brain with its defect and abstraction, the internet never forgets almost everyone and everything so far information is digitally onboarded. [116]Information is constantly and endlessly available. The territoriality principle based solely on jurisdiction has become less evident, Article 3(2)a of the GDPR brings non-EU data controllers and processors under the GDPR when they process EU citizen's data. [117]However, it is difficult to admit that a non-EU based company is subjected to EU law because EU citizen make use of the company's services. [118]In the absence of a harmonizing data protection law, the Chinese terms are not congruous, which embroil their application[119]. [120]Due to the inconsistency in the Chinese terms, the nearest definition of the EU controller is called 'internet service providers', 'internet information service providers', 'information controllers', 'personal information controllers', 'network operators' and 'information processing subjects',[121]while the closest definition to EU processors is referred to as the 'persons trusted with the processing' and 'personal information recipients'.

---

[109] Ibid.,
[110] Zhao, B., & Chen, W. (2019). Supra notra 13, 98
[111] Michael Laforgia, Gabriel J.X Dance (2018), Facebook gave data access to Chinese firm flagged by US intelligence, New York Times
[112] Ibid., 113
[113] Zhao, Bo & Chen, W (2019). Sopra notra 13. 98
[114] Rustad, Michael L. and Kulevska, Sanna (2015), Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow. Harvard Journal of Law and Technology, Vol. 28, p. 349, 2015, Suffolk University Law School Research Paper No. 15-27,
[115] Ibid., 116
[116] Viktor Mayer-Schonberger, (2009), Delete: The Virtue of Forgetting In The Digital Age, pg 118
[117] European Commission https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en
[118] Geller (2020). Supra notra 20, 1194
[119] Ibid., 120
[120] Cheng, 'Civil Liability' (n 6) 40
[121] Civil Code, arts 1036, 1038; Standardizing Regulations 2012, art 4; Decision 2012, art 2; Guidelines 2013, art 3.4; Standard 2020, art 3.4; CSL, art 76(3); Draft Administrative Measures, art 38(1); Draft Law, art 44(2).

2.3. Right To Be Forgotten

Some other concepts introduced by the GDPR are building on EU case law. [122]The right to be forgotten in the regulation extends the conventional data subject's right of erasure by requiring the controller or processor to forward erasure requests to all recipients of personal data. [123]One of the critical aspects of the data processing directive is that of the consent of the data subject. [124]Without the consent of the data subject, data controller is not privileged to perform any activities in majority of the situations, so far it falls under collective term of processing in the language of the data processing directive. [125]The RtbF has risen to prominence alongside the rising significance of privacy law in general, the RtbF is inherently the concept that data subject has the right to request that their data be deleted [126]. In 2014, the ECJ held in favour of the Spanish citizen (C-131/12). [127]The court stated that, according to the Article 4.1 (a) of the directive 95/46/EC, [128]the European Data Protection Directive applies to internet search engine operators if one or more of the three conditions set aside are fulfilled. In China, there are deep concerns regarding issues around internet users' online privacy and data security being the most populous nation on earth. [129]The key players in the internet world, specifically in relation to personal data are Facebook, Google, Twitter, and Microsoft. There are unauthorized avenues of data leakage on

[122] Eugene, Alexandra, Efthimios, Mattias, Constantinos (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. Computer Law & Security Review. Vol 34, Issue 6, pg 1248

[123] Cesare, Lawrence (2016). The right to be forgotten in the light of the consent of the data subject. Computer law & Security Review. Vol 32, Issue 2, pg 220

[124] Ibid., 125

[125] Eduard, Peter, Tiffany (2018). Human forget, machines remember: Artificial intelligence and the Right to be Forgotten. Computer Law & Security Review. Vol 34, Issue 2, pg 305

[126] 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).

[127] Court of Justice of the European Union (2014) C-131/12 Google Spain SL, Google Inc v. Agencia Española de Protección de Datos(AEPD), Mario Costeja González. Available at: curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.305computer law & security review 34, pg 304–313

[128] 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

[129] Bernal, P.A., 'A Right to Delete?', European Journal of Law and Technology, Vol. 2, No.2, 2011

Facebook's data platform despite correct policy specifications by its users[130]. [131] With the public data erasure obligation and considering the state of technology and the cost of implementation, the data controller has the obligation to take appropriate steps which include technical measures of informing the data processors of the data subject request and to delete any copy or link or replication of such personal data. [132]Nevertheless, according to article 17(3), the Regulation allows for some exemptions from the "forgetting" requirement, e.g., cases such as compliance with an obligation or in the exercise of controller's official authority. [133] Limiting de-listing to EU domains because users tend to access search engines via their national domains cannot guarantee the rights of data subjects. [134]The RtbF apparently takes a proprietary approach to privacy protection. [135] Data controllers invoke the anonymization argument as their major line of defense. [136]Formally acknowledging right in the GDPR signifies democratizing something private companies were exploiting at data subject's expenses. [137] *The Google Spain SL and Google Inc. v. AEPD and Costeja Gonzalez* ruling, Google created an elementary framework. A new online form was also created for data subjects to make requests for removal of links to online content, however, a reason for removal must be stated. [138]The Regulation stipulates that when someone demands the erasure of personal data, it is compulsory that an Internet Service Provider shall carry out the erasure without delay,[139]unless the retention of data is necessary to justify the right of freedom of expression. China[140] introduced a right to delete and correct in its article 43. GDPR permits data subject to request for erasure of its data regardless it's the era of machine learning, the CCL permits the controller to correct or delete personal information of data subject on the circumstances that the data was inaccurate or unlawfully collected.

[130]Patil V.T., Shyamasundar R.K. (2018) Efficacy of GDPR's Right-to-be-Forgotten on Facebook. In: Ganapathy V., Jaeger T., Shyamasundar R. (eds) Information Systems Security. ICISS 2018. Lecture Notes in Computer Science, vol 11281. Springer, Cham

[131] Eduard, Peter, Tiffany (2018). Supra notra 127, 306

[132] Eugene, Alexandra, Efthimios, Mattias, Constantinos (2018). Supra notra 124, 1249

[133] J Powles. (2015) 'The case that won't be forgotten', 47 Loyola University Chicago Law Journal, pg 583

[134] J Ausloos (2012). The 'Right to be Forgotten' – Worth remembering? Computer Law & Security Review Volume 28, Issue 2, Pg 144

[135] Ibid., 136

[136] Eduard, Peter, Tiffany (2018). Supra notra 127, 306

[137] Voss, W. Gregory (2014), The Right to Be Forgotten in the European Union: Enforcement in the Court of Justice and Amendment to the Proposed General Data Protection Regulation (July 2014). Journal of Internet Law. Vol. 18, pg 5

[138] Jeffrey Rosen (2012), "The Right to Be Forgotten", 64 Stanford Law Review Online. Vol 64, pg 90

[139] Ibid.,140

[140] Meihui Zhang. (2020) Is There a 'Right to Be Forgotten' in China? Judicial Response to China's Tort Law on Privacy and Data Protection Issues. Forthcoming in Consumer Protection in China: Current Challenges and Future Prospects pg 14

3. PROPOSAL TO AMEND CCL TO GDPR STANDARDS

While I completely agree that the Chinese have taken drastic measures to be compliant with the responsibility of Extraterritoriality, meeting the standards of GDPR is not imminent. China is the largest trade partner with the EU, as such, the mission of adopting GDPR model should be given more attention and concern. The terminology "consumer" regarding owner of data as portrayed in China should be classified as data subject. While individual can be a consumer, which is someone that exchange good or services with no commercial ulterior. Compliant with GDPR is major force to reckon with, China published a draft of a new law with borrowed idea from GDPR. [141]Once announced, Data Security Law and Cybersecurity Law will be a fundamental law with the Personal Information Protection Law published on Oct. 21, 2020. This further corroborates the lack of standard approach as China has struggle to get it right with data protection. Successful transition between data protection laws can form a standard model which can hasten the integration of GDPR extraterritoriality, however, churning out different rules while previous laws are yet to reach its full potential will only spell doom for subsequent ones. Take for instance, the data protection Directive ran its full course prior to its transition into GDPR. More importantly, its guarantee the data protection and privacy of European residents regardless of the location their data is being processed.

Despite frantic efforts of the Chinese government to steadily build out its data privacy system via the release of the Personal Information Security Specification in May 2018[142], having relied on scattered provisions. These provisions lack harmonization with the Chinese government thereby restricting legislative capacity in the system[143]. The EU had a long-standing bearing and plan of action regarding data privacy and data protection prior to enactment of data privacy rules in China. If China toured the blueprint of EU GDPR rather than a scattered data privacy rule, EU extraterritorial application in China would experience a positive adoption model of high compliant standards. The Chinese data protection trajectory seems immediate when compared to the U.S. outlook. For instance, the notification of data breach requirements in America is not as scrupulous when compared with the EU. Whenever a data breach happens, the notification stipulation compels the unit in charge of the data to alert the relevant

[141] George Qi. (2021). China Releases Draft Personal Information Protection Law
[142] Alexa Lee. (2021). Personal Data, Global Effects: China's Draft Privacy Law in the International Context
[143] Ibid.,

authority and the individuals. In U.S., it can be up [144]30 days or perhaps up to a reasonable time. The EU data breach notification obliges data controllers to alert the supervisory authorities of a breach within the next 72 hours of awareness[145], the rules goes further than both the U.S. and OECD. CCL necessitate data controllers to notify the supervisory authorities as well as data subjects in a situation of data breach. The unit affected must record specific information regarding the breach, impact must duly assess and promptly reported. However, the Chinese rules did not explicitly elucidate the term "promptly"[146].

The GDPR is enforced by independent authority that provides regulatory supervision, however, CCL lacks an established independent regulatory oversight dedicated to data privacy enforcement[147]. There are many supervisory authorities in U.S. charged with responsibility of enforcing privacy provisions, which proves CCL approach is like that of U.S. So far, the most successful Chinese data rule is CCL, I believe the amendment of CCL towards GDPR standards will ensure clarity for companies that process both Chinese and European resident's data.

[144] See Colorado Consumer Data Privacy Law Sec.3 (2)
[145] GDPR, Article 33(1)
[146] China's Cybersecurity Law, Art 42
[147] Emmanuel Pernot-Leplay (2020). Supra notra 73

The proposed process and outcome are illustrated below.

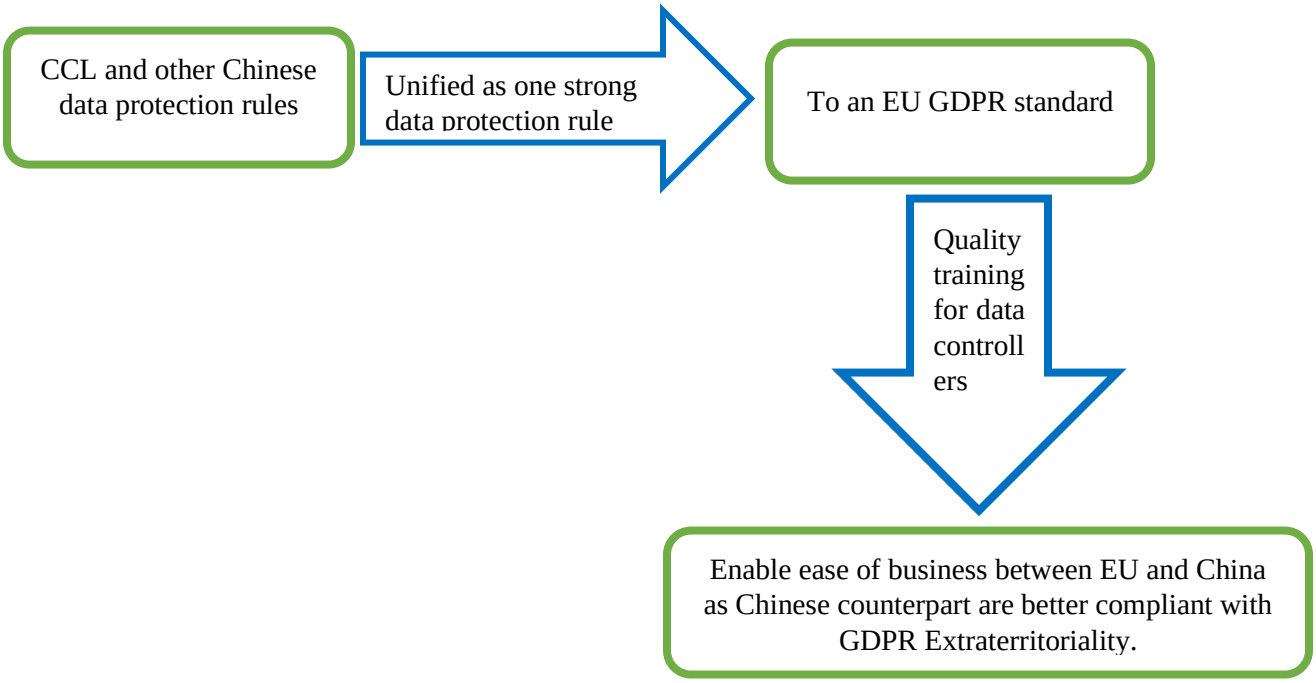


Fig 1. The proposed process and outcome of a uniform amended China Cybersecurity Law

A harmonized single legal document of data protection with GDPR standard will significantly influence the processing of data.

In conclusion, data controllers can cope easily by dealing with straightforward data protection rules, as compared to struggling on different fronts and trying to create a balance. The moment CCL is aligned with GDPR, controllers can proactively ensure full compliance which will become more symbiotic and generates a promising result towards Extraterritorial adoption of GDPR.

3.1 Recommendation for High-Minded Training Models to CCL/GDPR Standards

Business owners in China that process the data of EU residents must consider that GDPR compliance requires valuable and significant legal experience and proficiency. It is highly recommended for [148] business ties with EU to seek local legal assistance to avoid facing the wrath of GDPR Extraterritoriality. A Data Protection Officer (DPO) role might come in handy for organizations that process large amount of EU resident's data in China. DPO is responsible for supervising a company's data protection implementation and strategy to ensure adequate compliance with GDPR requirements[149]. The role of a DPO is vital where the core activities of the controller entail systematic and ongoing monitoring of data subjects on a large scale or in a situation where personal data is processed on special categories such as ethnicity, religious belief, or race[150]. According to Article 37 of GDPR, companies that collect and process personal data of EU residents must have a DPO to help with regular security checks, staff training regarding data processing and educating employees on significant compliance requirements[151]. Hiring a professional DPO pose adjustment investment cost, however, compliant with the Regulation is much safer as compared with the risk of being fined for violation. Once the CCL is upgraded to the GDPR standard, the DPO will be responsible for bringing the company to speed by developing and implementing procedures and policies that are in line with the data protection Regulation.

[148] Michael Tan. (2018), Supra notra 1
[149] Nate Lord. (2020). What is a Data Protection Officer (DPO)? Learn About the New Role Required for GDPR Compliance in 2019.
[150] Ibid.,150
[151] Ibid.,

CONCLUSION

The research aimed to explore the adoption of GDPR extraterritoriality in China, to identify how data controllers and processors can effectively be compliant with the Regulation to strengthen the business activities between the EU and China. The landscape of CCL and other sparsely data protection laws in China has proven to be insufficient as the standards fell short of GDPR model. Therefore, increased challenges for data protection have emerged and due process is not obtainable. The predominant factor of the inadequacy concerns the legal awareness and extraterritorial scope on how to adopt GDPR mechanisms effectively due to lack of knowledge of the procedures. A comparative analysis was applied between the EU GDPR and China's CCL to establish the status quo obtainable currently and observe the landscape of GDPR. It was discovered that the transition of a consistent approach in data processing invigorates GDPR as a better form of data protection law in EU in contrast to more scattered approach in China. By adopting GDPR standards, Chinese controllers will have to contend with a specific data protection mechanism rather than being sceptical about different data protection and privacy rules. The evidence proved some Chinese companies have the capacity to be complaint with GDPR despite the investment cost, however, failure to show same level of complaint towards CCL might be disastrous. In the case of an identical laws or adoption of GDPR, the focus of data controllers would be simplified. The EU had a well-established plan and preliminary strategy of data protection and privacy foregoing before the enactment of data privacy rules in China. The extraterritoriality of the GDPR enforced a tremendous responsibility on data controllers in China with high level of compliance. Perhaps China should imbibe the rich fundamental human right enshrined in EU laws because this has proved to be the foundation of the right to data protection. When the rights of the citizens are limited, it undermines the freedom which everyone should naturally enjoy.

The introduction of artificial intelligence (A.I) in training model for data controllers and processors in China will intensify data privacy and processing. To prioritize data protection, A.I requires a substantial proportion of regulation as it is closely related with big data. The Chinese counterpart must adopt the use of A.I to match the level of compliant required by GDPR. Arguably, A.I is developing in a fast pace globally as it ensures efficiency to a high-quality standard. Combination of data protection with A.I will significantly improve the effectiveness of data processing, especially in a situation where the company process lots of personal data. Integrating A.I into CCL will ensure a centralized model where DPO and controllers in China can obliterate the discrepancies associated with complications in processing of personal data. The author analysed and compared the adoption model of GDPR by the Chinese government, while there have been significant steps to adhere with the rules by companies, the Chinese government swerved towards the U.S model of adoption. In a situation of data breach, GDPR encourages swift intervention and notification both to the authorities and data subject, the timely intervention shows genuine concern and the profundity of data. The U.S authorities and the data subject are notified within a reasonable time after which unimaginable harm has occurred. The GDPR frowns at such recklessness, the author opined China should emulate such policy considering the amount of transborder data exchange between the two territories, especially on business related activities. The thesis clarified how restrictive privacy protection caused fundamental problem because Chinese privacy rules lacks extensive data protection design. Transparency and accountability are required regarding collection and processing of personal data to ensure trust from both sides. GDPR with its extraterritorial scope application avails data subjects an avenue of hope and guarantees utmost secured platform from anywhere in the world. CCL is widely assumed as the most prolific adoption model of GDPR, nevertheless, it lacks vital legal ingredients with restrictive tendencies. An imminent approach to GDPR standards would have been desirable, especially for data controllers trying to avoid fines from both the EU and Chinese government.

Data is regarded as the new oil; the author certifiably encourage an extreme measure to safeguard such value. Technological advancement dramatical increased online presence for numerous purposes in which business is an integral part. The sparse data protection law in China corroborates the view of Dr. Solarte-Vasquez who believe there are already too many laws and proffer a reform of existing laws. The amendment of CCL to GDPR standard as the only data protection law will not only integrate GDPR extraterritoriality with companies in China, however, it will further strengthen the trust of EU residents thereby creating a secured and trusted cross-border transaction.

LIST OF REFERENCES

Scientific Book

1. Bygrave, L., (2014) Data Privacy Law: An International Perspective, *Oxford University Press*, Oxford, pg 2057-2058

2. MAYER-SCHÖNBERGER, V. (2009). *delete: The Virtue of Forgetting in the Digital Age.* Princeton: Princeton University Press.

3. Vishwas, P. T., & Shyamasundar, R. K. (2018). *Efficacy of GDPR's Right-to-be-Forgotten on Facebook.* Bangalore: Information System Security.

Scientific Journal

1. Adele, A. (2018). The challenges faced by the extraterritorial scope of the general data protection regulation. . *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 126.

2. Alessandro, M. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review*, 229-235.

3. Ausloos, J. (2012). The 'Right to be Forgotten' – Worth remembering? *Computer Law & Security Review*, 144.

4. Bernal, P. A. (2011). A right to delete? *European Journal of Law and Technology*.

5. Birnhack, M. D. (2008). The EU Data Protection Directive: An engine of a global regime. *Computer Law & Security Review*, 551.

6. Burri, M., & Schar, R. (2016). The Reformof the EU Data Protection Framework: Outline Key Changes and Assessing Their Fitness for a Data-Driven Economy. *Journal of Information Policy*, 480.

7. Davies, S. (1996). *"Big Brother: Britain's web of surveillance and the new technological order"*. Pan.

8. Eugenia , P., Alexandra, M., Efthimios , A., Matthias, P., & Constantinos, P. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*, 1248.

9. Feng, Y. (2019). 'The Future of China's Personal Data Protection Law: Challenges and Prospects. *Asia Pacific Law Review*, 62-82.

10. Geller, A. (2020). How Comprehensive Is Chinese Data Protection Law?a Systematisation of Chinese Data Protection Law from an European Perspective. *GRUR International*, 1191.

11. Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. *International Data Privacy Law*, 72.

12. Hoecke, M. V. (2015). Methodology of Comparative Legal Research. *Law and Method*, 8.

13. I. VAN, O., & Helena U., V. (2019). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy*, 91.

14. Krystlik, J. (2017). With GDPR, Preparation is Everything. *Computer Fraud & Security*, 5.

15. Kuner, C. (2015). The European Union and the Search for an International Data Protection Framework. *Groningen Journal of International Law*, 64.

16. Lawrence, C. (2016). The right to be forgotten in the light of the consent of the data subject. *Computer Law & Security Review*, 220.

17. Meihui, Z. (2018). Is there a 'Right to be Forgotten' in China? Judicial Response to China's Tort Law on privacy and data protection issues. *Nankai University*, 14.

18. Mikkonen, T. (2014). Perceptions of controllers on EU Data Protection Reform: A Finnish Perspective . *Computer Law and Security Review*, 190-195.

19. Nate Lord. (2020). What is a Data Protection Officer (DPO)? Learn About the New Role Required for GDPR Compliance in 2019

20. Paul de, H., & Vagelis, P. (2016). The New Police and Criminal Justice Data Protection Directive: A First Analysis. *New Journal of European Criminal Law*, 130-142.

21. Pernot-Leplay, E. (2020). Data Privacy Law in China: Comparison with the EU and U.S. Approaches. *Penn State Journal of Law and International Affairs* , 51.

22. Poullet, Y. (2006). EU Data Protection Policy. The Directive 95/46/EC: Ten years after. *Computer Law & Review*, 211.

23. Powles, J. (2015). 'The case that won't be forgotten'. *Loyola University Chicago Law Journal*, 583.

24. Reding, V. (2019). The upcoming data protection reform for the European Union. *International Data Privacy Law*, 3.

25. Rosen, J. (2012). “The Right to Be Forgotten. *Stanford Law Review Online*, 90.

26. Ryngaert, C., & Taylor , M. (2020). The GDPR as Global Data Protection Regulation? *AJIL Unboud*, 6.

27. Sloot, B. V. (2014). Do Data Protection Rules Protect The Individual and Should They? An assessement of the proposed General Protection Regulation. *International Data Privacy Law*, 307.

28. Tiffany, L., Eduard , V. F., & Peter, K. (2018). HUMANS FORGET, MACHINES REMEMBER: ARTIFICIAL. *Computer Law & Security Review*, 305.

29. Tikkinen-Piri, C., Anna , R., & Jouni , M. (2018). EU Genenral Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 134.

30. Victor, J. M. (2014). The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy. *The Yale Law Journal*, 513.

31. Voss, W. G. (2015). The Right to Be Forgotten in the European Union: Enforcement in the Court of Justice and Amendment to the Proposed General Data Protection Regulation. *Journal of Internet Law*, 5.

32. Yang, F., & Jian, X. (2018). Privacy concerns in China's smart campaign: The deficit of China's Cybersecurity Law. . *Asia and the Pacific Policy Studies*, 538.

33. Zhao, B., & Chen, W. (2019). Data protection as fundamental right: The european general data protection regulation and its exterritorial application in china. *US-China Law Review*, 97.

34. Zhao, B., & G.P Jeane, M. (2016). Protecting EU citizens' personal data in China: a reality or fantasy? *International Journal of Law and Information Technology*, 128-150.

Other Sources

DEFINITIONS. (n.d.). Retrieved from https://www.definitions.net/definition/data.

Garrelfs, A. (n.d.). Retrieved from Deloitte: https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-extraterritorial-applicability.html

Hustinx, P. (2013). EDPS Speeches & Articles, EU Data Protection Law: The Review of Directive 95/46/EC and The Proposed General Data Protection.

Huang, E. W. (2018). Eric W. Huang. (2018). China: An overview of China’s New Cybersecurity Law.

JOURNAL, C. B. (2019, May 24). Retrieved from LAWdotASIA: https://law.asia/the-impact-of-eus-gdpr-in-china/

KPMG. (n.d.). Extraterritorial scope of the GDPR. *The Impact of the GDPR on Organizations in Asia*.

Leo, Z., & Lulu, X. (2018, March 1). *CHINA BRIEFING*. Retrieved from https://www.china-briefing.com/news/chinas-cybersecurity-law-an-introduction-for-foreign-businesspeople/.

Michael, L., & Gabriel, D. J. (2018, June 5). *Facebook gave data access to Chinese firm flagged by US intelligence, New York Times*. Retrieved from New York Times: https://www.nytimes.com/2018/06/05/technology/facebook-device-partnerships-china.html

Nadeau, M. (2020, June 12). Retrieved from CSO.

OECD. (2000). *"Transborder Data Flow Contracts in the.* Paris: OECD Digital Economy Papers.

Prud'homme, D., & Zhang, T. (2019). *China's Intellectual Property Regime for Innovation.* Paris, Shanghai: Springer.

Qi, G. (2021, January 21). China Releases Draft Personal Information Protection Law.

S, Y. Y. (2018). The impact of the GDPR and China's data protection regime towards Chinese cloud service providers with regards to cross-border data transfers. *Master's Thesis, Tilburg University, Tilburg Law School*, 9.

Shi, Y., & Jared, N. T. (2018, May 31). Retrieved from https://www.ofdigitalinterest.com/2018/05/the-gdprs-effects-in-china-comparison-with-local-rules-and-considerations-for-implementation/.

Tan, M. (2018, July 18). Retrieved from TaylorWessing.

Vitcheva, D. (2019, August 14). Retrieved from transcendent group: https://transcendentgroup.com/news/myths-on-the-extraterritorial-scope-of-the-gdpr/.

CASE LAW

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12 (Court of Justice of The European Union (CJEU) May 13, 2014).

LEGISLATIONS

Article 1(1)(b) of the GDPR. (n.d.).

Article 3 of the GDPR sets out the two limbs of the territorial scope. The first being where data processing activities are conducted by organisations (controller or processor) established in the EU - a principle established under European case law when i. (n.d.).

Article 58 of the GDPR. (n.d.).

Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1. (2000).

Cheng, 'Civil Liability' (n 6) 40. (n.d.).

Civil Code, Arts 1036, 1038. Standardized Regulations. (2012).

Civil Code, arts 1036, 1038; Standardizing Regulations 2012, art 4; Decision 2012, art 2; Guidelines 2013, art 3.4; Standard 2020, art 3.4; CSL, art 76(3); Draft Administrative Measures, art 38(1); Draft Law, art 44(2. (n.d.).

Commission, E. (n.d.). Retrieved from European Commission: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350/60, 30.12.2008. (n.d.).

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. (n.d.).

Handbook on European Data Protection Law edition. (2018). 28.

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 Da. (n.d.).

(n.d.). *Advocate General Sharpston described the case as involving two separate rights: the "classic" right to the protection of privacy and a more "modern" right, the right to data protection. See CJEU, Joined cases C-92/09 and C-93/02, Volker und Markus Schecke.*

APPENDICES

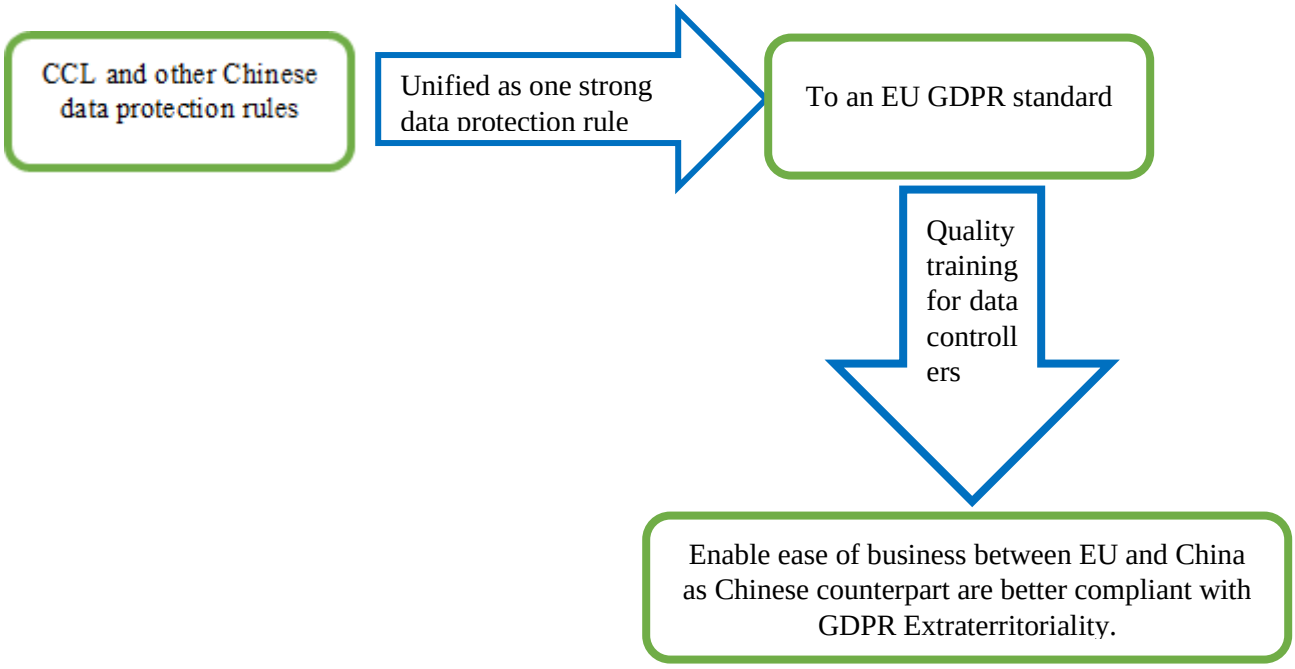
Appendix 1. Table 1. Comparison between General Data Protection Regulation and Chinese rules

Item	GDPR	Chinese Rules
Key Categories of Entities	Data Controller Data Processor Data Recipient	Network Operator Network Product/Service Provider Critical Information Infrastructure Operator Personal Information Controller Personal Information Processor
Age for Protection of Children	16 years old	14 years old
Right To Be Forgotten and Deletion Right	Data subjects have the fundamental right to acquire from the controller the erasure of personal information in several conditions, including where: (a) the personal data is no longer necessary in relation to the purposes for which it was collected or[152] otherwise processed; or (b) the data subject withdraws consent and there is no other ground for the processing.	Data subjects have the right to obtain from the controller the erasure of personal information in several conditions, including where: (a) controllers violate provisions of the laws and regulations in collecting or using personal information; or (b) controllers violate agreements with the data subject in collecting or using personal information.

Source: Jared Nelson and Shi Yuhang. (2018). China: The GDPR's Effects in China: Comparison with Local Rules and Considerations for Implementation.

[152] Ibid.,

Appendix 2. The proposed process and outcome of a uniform amended China Cybersecurity Law



Appendix 3 Non-Exclusive License

A non-exclusive license for reproduction and for granting public access to the graduation thesis[153]

I Sodiq Itunu Saheed 26/06/1989

1. Give Tallinn University of Technology a permission (non-exclusive license) to use free of charge my creation

Extraterritorial Impact of the General Data Protection Regulation (GDPR), a case study of The Chinese Adoption Model

Supervised by Maria Claudia Solarte Vasquez

1.1. To reproduce with the purpose of keeping and publishing electronically, including for the purpose of supplementing the digital collection of TalTech library until the copyright expires.

1.2 To make available to the public through the web environment of Tallinn University of Technology, including through the digital collection of TalTech library until the copyright expires.

2. I am aware that the author will also retain the rights provided in Section 1.

3. I confirm that by granting the non-exclusive license no infringement is committed to the third persons' intellectual property rights or to the rights arising from the personal data protection and other legislation.

[153] The non-exclusive license is not valid during the access restriction period with the exception of the right of the university to reproduce the graduation thesis only for the purposes of preservation.