Data Adequacy and China

The possibility of an adequacy decision adopted on China in accordance with the GDPR Article 45

Kandidatnummer: 96

Antall ord: 13955

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

10.12.2019

Table of contents

List of abbreviations

CAC	The Cyberspace Administration of China
EEA	The European Economic Area
EU	The European Union
GDPR	The General Data Protection Regulation
ICO	Information Commissioner's Office
LIBE	The European Parliament's Committee on Civil Liberties, Justice and Home Affairs
PPC	The Personal Information Protection Committee of Japan
SAC	Standardization Administration of the People's Republic of China
TC260	The National Information Security Standardization Technical Committee of China
The Commission	The European Commission
The Council	Council of the European Union
The CSL	The Cybersecurity Law of China
The EDPB	The European Data Protection Board
The Measures	The Security Assessment of Cross-Border Transfer of Personal Information and Important Data of China

The Plan	The National Cybersecurity Incident Response Plan of China
The Standard	The Information Security Technology – Personal Information Security Specification of China
UK	The United Kingdom
US	The United States of America
WP29	Article 29 Working Party

1. Introduction

1.1 Topic of this Thesis

This thesis covers the possibility of passing a so-called "adequacy decision" on China in accordance with the General Data Protection Regulation[1] (GDPR) Article 45. This is done by conducting an assessment based on the evident legal criteria and the current Chinese data protection framework.

1.2 The Relevance of the topic

The GDPR entered into force on the 25th of May 2018. It replaced the Data Protection Directive of 1995[2] and introduced several changes to EU data protection law, including more stringent consent conditions, higher penalties for violations and an expanded territorial scope. In addition to providing improved protection for individual's personal data, the regulation was designed to harmonize the data protection rules within the EU as well as modernizing them in order to keep up with the present modern digital society.[3] A more in-depth review of the GDPR, its provisions and its territorial scope will be given in section 2.

This new and comprehensive set of rules implemented through the GDPR received close review internationally as data controllers and processors attempted to prepare for these new requirements. Due to the expanded territorial scope, the GDPR became applicable outside the EU zone in a larger scale than previous EU data protection legislation. This created uncertainty and confusion far beyond the borders of the EU. In fact, when the GDPR was implemented in May of 2018, several US websites became unavailable to EU users. The organizations behind the websites especially feared the fines imposed on breaches of the GDPR, which may be as high as 20,000,000 EUR or 4% of a company's annual turnover.[4] This makes GDPR compliance ever so relevant. High profile websites including New York Daily News, Chicago Tribune, Los Angeles Times and The Baltimore Sun were among the websites that became

[1] Regulation (EU) 2016/679 (henceforth GDPR)
[2] Directive 95/46/EC (henceforth Directive 95/46)
[3] GDPR Article 1
[4] GDPR Article 83

unavailable. Other major news outlets such as the Washington Post and the Times had EU users agree to new terms to guarantee compliance following the implementation.[5]

Simultaneously, numerous complaints were filed against US tech giants in the EU, accusing them of being in breach of the GDPR requirements. Among the accused were important companies such as Facebook, WhatsApp, Google and Instagram. The complaints were filed by "NOYB", a non-profit organization led by data protection activist Maximillian Schrems. The organization claimed that the companies forced users of their services to consent to data processing if they wanted to continue to use the services, in violation of the GDPR Article 7 (4).[6] These complaints showcase how the implementation of the GDPR immediately created effects outside the EU.

The upcoming withdrawal of the United Kingdom from the EU, commonly known as Brexit, also sheds light on the relevance of this topic. As a result of leaving the EU, the UK will also become a third country[7] in accordance with the GDPR. They will therefore need an adequacy decision in order to exchange personal data on the same terms as the remaining EU countries.[8]

1.2.1 The importance of an adequacy decision

Creating a digital "global village"[9] consists of a compromise between the protection of personal data on one side and information sharing, cross-border business and trade on the other. Through the adoption of adequacy decisions, the EU attempts to ensure that the stringent personal data protection rules within the EU follow the data when it is transferred to a third country. This is also affirmed in the GDPR recital 6. Additionally, adequacy decisions make it easier for the EU

---

[5] BBC News, "GDPR: US news unavailable to EU users under new rules"
[6] NOYB (2018)
[7] Any country or territory outside of the EU/EEA. (The European Economic Area (EEA): an agreement between the EU, its Member States and the three EFTA-countries Norway, Lichtenstein and Iceland. It extends the EU's single market to also include these three countries.)
[8] ICO, Denham (2019);
The Information Commissioner's Office (ICO) has expressed that obtaining an adequacy decision after Brexit is the plan. This will however take a couple months at minimum as the adequacy assessment is unable to start before the UK leaves the EU and officially become a third country. The ICO has therefore issued several guidelines for smaller and bigger companies to maintain GDPR compliance when Brexit becomes reality.
[9] "Global village" was a term introduced by Herbert Marshall McLuhan in his 1960s works. The term is used to describe a world becoming interconnected by the means of media and technology. Cambridge Dictionary defines #the global village" as "countries being closely connected by modern technology and trade".

and its institutions to collaborate outside the Union regarding investigations and cross boarder crime, which is essential in an increasingly digital society.

Without an adequacy decision, third countries and organizations are unable to benefit from the free flow of data. In order to transfer personal data lawfully without an adequacy decision, organizations will have to apply alternative tools for transfers in accordance the GDPR Chapter 5, which involves more complicated and cumbersome processes. Ultimately, an adequacy decision intertwines the country or territory in question to the free flow data market within the EU-zone.

1.2.2 The relevance of an adequacy decision with China

As this thesis aims to account the possibility of an adequacy decision with China, it is important to understand why this in particularly would be beneficial. As already stated, the territorial scope of the GDPR expands outside EU borders. This forces institutions and companies outside the EU area to comply with the rules of the GDPR, if the specified requirements mentioned under subsection 2.2 are met.

With China being one of the largest economies in the world, an adequacy decision on China would make trade and other cross-border commerce more efficient. In fact, the EU is the biggest trading partner of China, and China the second biggest of the EU, only succeeded by the United States of America (US). The average daily trade between China and the EU is estimated to be 1 billion EURO according to the European Commission (the Commission).[10] The amount of trade and commerce with China further amplifies the need for an adequacy decision.

This would ease the personal data exchange of international companies with branches in both the EU and China, or Chinese companies who for example wish to offer their services though an app targeting EU residents. The absolute simplest, cheapest and least time-consuming way for them to go about processing of personal data would be though an adequacy decision.

[10] EC, “China”

1.3 Methodology and legal sources

As this thesis is based on a GDPR provision, which is an EU regulation, and it is within the GDPR the legal basis for adequacy decisions are found, the thesis statement will be based on EU legal method. EU law is an autonomous legal system and there is a specific EU legal method to be applied while assessing legal issues within this jurisdiction. This method is established by the practice of the Court of Justice of the European Union (CJEU), who also have the exclusive right to interpret EU legislation. The main traits of this method are that the interpretation shall be in conformity with the wording of the provisions and stay true to the relevant objections. The CJEU has concluded that "in order to determine the scope of a provision of EU law, its wording, context and objectives must all be taken into account".[11]

EU legislation will be used to establish the legal framework of EU data protection law, most importantly the GDPR, Directive 95/46 and the already existing acts on adequacy decisions passed by the Commission. The decision on Japan[12] will be particularly in focus as it is the one most recently adopted as well as the only one with its legal basis in the GDPR. In addition to the Commission acts implementing adequacy decisions, other Commission soft law such as press releases and guidelines are used as they impact the policy development and practice.[13] The official Commission website will also be used as a reference as it expressed the official opinion of the Commission. Although it is not an official legal source, the information expressed on the website will be of relevance as the Commission is the institution conducting the adequacy assessments and implementing the decisions.

Judgements from the CJEU will be used to clarify the matter substance of the GDPR Article 45. As the GDPR is still relatively new, most judgments concerning adequacy decisions are based on the previous legal basis for adequacy decisions in Article 35 (6) of Directive 95/94, which contained the corresponding term "adequate level of protection". As this provision has been carried on from Directive 95/46 to the GDPR, the judgements are still applicable to interpret the current provisions. Despite the Commission being the executive power within the EU, the CJEU determines the prevailing law.

---

[11] *Azevedo and Others*, C-558/15, para. 19.
[12] (EU) 2019/419
[13] Soft law is used to describe opinions, guidelines, declarations etc. that are not legally binding as opposed to hard law which refers to legally enforceable obligations such as legal acts, regulations, directives and decisions.

Guidelines and other documents issued by the European Data Protection Board (EDPB) are also of relevance in order to assess the data adequacy situation in China. The EDPB is responsible for ensuring "the consistent application of the Regulation" in accordance with the GDPR Article 70 (1). This includes making sure data protection law is applied consistently throughout the EU, ensure cooperation between the national Data Protection Authorities, issue guidelines on the interpretation of the GDPR and to issue binding decisions in cases of cross border processing disputes. Ultimately, the task of the EDPB is to ensure conformity across the EU under the rule of the GDPR. They issue documents essential to understanding the interpretation of the GDPR provisions, including elements of particular importance in regard to adequacy assessments. Also, documents issued by the EDPB's predecessor, Article 29 Working Party (WP 29) are good references for clarification and summaries of the prevailing law based on relevant case law, procedure and internal instructions.

The EDPB is to act independently and without taking instructions but does nevertheless have an advisory role towards the Commission. In addition to examining any question concerning the application of the GDPR on its own initiative, this should also be done on request from members of the Commission. The EDPB is also to advise the Commission on any issue regarding data protection within the EU, on any proposed amendment to the GDPR. More important for the assessment of data adequacy, the EDPB is required to provide the Commission an opinion regarding the adequate level of protection in a third country during such a process.[14] This proves the importance of EDPB sources for this thesis regardless of the limited legal weight.

Concerning the Chinese legal framework, the most important regulations are the Cybersecurity Law (CSL) and the Information Security Technology - Personal Information Security Specification (the Standard). The CLS is a formally enacted law, while the Standard is a set of voluntary guidelines. They are however adopted pursuant to the CSL, and its provisions are regarded as an extension of the cybersecurity system set out by the CSL. The Standard accordingly intends to provide a more in-depth and detailed understanding of the personal data legal framework. They will be used intertwined to give an image of the Chinese data protection framework as a whole.

[14] EDPB, "Role of the EDPB"

For all EU sources, the official English version will be used. In absence of official English translations, unofficial translations of the Chinese legislation will be used. The translations are necessary as I am not proficient in Chinese and therefore not able to use the official Chinese versions for the assessment.

1.4 The relevant notions

This section will briefly specify some of the relevant notions that will be used in the thesis. As the Chinese framework does not operate with the equivalent terms as the GDPR, it is necessary to establish the differences and/or similarities to avoid ambiguity in the further portrayal.

1.4.1 Personal data

The definition of "personal data" is given in GDPR Article 4 (1). It states that "any information relating to an identified or identifiable natural person [data subject]" is included. It further specifies information such as "names, dates of birth, identity card number, biometric information, addresses, telecommunication contract methods, communication records and contents, account passwords, property information, credit information, location data, accommodation information, health and physiological information, transaction data, etc." as elements to consider particularly, although this list is not meant to be exhaustive.[15]

In contrast the Standard use the term "personal information", which is defined as "All kinds of information, recorded by electronic or other methods, that can be used, alone or combined with other information, to identify a specific natural person or reflect activities of a specific natural person".[16]

Both frameworks give a clear definition of what is regarded as respectively "personal data" in the GDPR and "personal information" in the Standard. The two definitions are not identical, but the intentions of the two do however correspond to a large extent. The essence of both definitions seems to be the possibility of identification, either by the concrete data itself or combined with other available data. Due to the concurrent objectives of the two definitions, the

[15] GDPR Article 4 (1)
[16] The Standard Article 3.1

GDPR's term "personal data" will be used throughout the thesis to cover both definitions.

1.4.2 Processing of personal data

The term "processing" will be used for operations performed on personal data, automated or not, including collection, storage, recording etc., in accordance with the GDPR Article 4 (2). In the introduction of the Standard it is stated that its purpose is to regulate behavior related to "information processing such as collection, retention, use, sharing, transfer, and public disclosure".[17] The term processing is furthermore used frequently in the provisions of the Standard in addition to in Chapter IV of the CSL, suggesting a corresponding meaning in the Chinese framework. An example of processing would be storing the IP address of people visiting your website.

1.4.3 Controller

The GDPR defines a controller as a "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data".[18] In the Chinese framework, the term "Personal Information Controller" is used, which is defined as "an organization or individual that has the authority to determine the purpose and/or methods of processing PI [personal information]".[19] Summarized by these definitions, a controller will be any individual, company or organization determining how and when personal data is to be processed. This may for example be a company collecting personal data from their employees.

1.4.4 Processor

A processor is defined in the GDPR as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".[20] These organizations process personal data on behalf of a controller but are nevertheless required to ensure GDPR compliance. A typical example of a data processor is when companies offer IT services such as for example cloud servers and payroll services to other organizations acting as controllers.

---

[17] The Standard - Introduction
[18] GDPR Article 4 (7)
[19] The Standard Article 3.4
[20] GDPR Article 4 (8)

The Chinese framework does not operate with a concurrent term. All requirements are directed at controllers because they are the ultimate responsible party to ensure data protection. Because there is no definition, the presumption is that processors are not subject to the Standard. The fact that processors are not defined does however not mean that the Standard excludes the use of third parties conducting such tasks. Controllers deciding to use third parties for processor-activities in China will however have to pay more attention to who they enter into contract with as they will be held responsible for lack of compliance.

1.4.5 Transfer to third country

An adequacy decision is a way of safeguarding the transfer of data to a third country, which makes it relevant to clarify this term. The term refers to the transfer of personal data currently undergoing processing or intended for processing in the third country. It is not a requirement that the data is transferred physically to the third country. The fact that a subject in a third country can access a server containing the personal data, even if this server is placed within the EU, is enough for a transfer of data to have occurred in accordance with the GDPR. It will also be considered a transfer where a subsidiary company located within the EU transfers personal data to a parent company located in a third country[21]. An example would be if an EU company that offers trips to China provided the costumer's booking information (including details such as names, passport information, social security number, date of births, etc.) on to the hotel in China. Such a transfer can only take place in the event of an adequacy decision or other safeguards in accordance with the GDPR for the transfer to be legal.

Information on a website that is based within the EU, but makes the information available to third parties in third countries, will not be regarded as a transfer in accordance with the *Lindqvist*-judgement.[22] Neither will the routing of personal data between two EU countries (or a third country with data adequacy) through a server in a third country, if the personal data in question is not intended to be accessed in the third country. This is categorized as "transit" and will fall outside of the scope of thesis.

[21] Udsen, (2019), p. 436-438
[22] *Lindqvist*, C-101/01, paras. 52-71

1.4.6 Recipient

The GDPR defines a recipient as any "natural or legal person, public authority, agency or another body, to which the personal data are disclosed" in Article 4 (9). Whether this is a third party or not is insignificant. The provision does contain an exception for public authorities receiving personal data in accordance with EU or national law, but this exception will not be addressed further. The term is neither defined in the CSL nor the Standard yet is referred to in several provisions. For example, controllers are to "notify recipients to delete the information" in the event of unlawful disclosure of personal data.[23] Although the term in not explicitly defined, the way it is used in the provisions of the Standard indicates a similar meaning as that of the GDPR, that being someone who has received the relevant personal data in question.

1.5 Structure of the Thesis

In the following segment there will be three main sections. The first will give a brief and general introduction to the GDPR and its objectives, as well as a short introduction to the territorial scope, with focus on how and when the regulation becomes applicable for entities located in third countries such as China.

Secondly, there will be given an introduction to the concept of an adequacy decision as well as the procedure and legal criteria required for the Commission to implement such an act. The most recent adequacy decision adopted on Japan will be used as a reference to see how an adequacy assessment is conducted in practice.

In the third section contains the main portion of the thesis, which will provide an attempt to form a picture of the current status of data adequacy in China by looking at some of the central provisions in the legal framework, in addition to enforcement and supervision mechanisms. Some of the differences between the Chinese framework and the GDPR will also be highlighted, as well as additional observations relating to China's data adequacy.

[23] The Standard Article 7 (6) c)

1.6 Limitations

The thesis will be limited to adequacy decisions in GDPR Article 45, meaning that other provisions of transfers to third countries in the GDPR will be excluded. A short section elucidating the criteria for application based on GDPR Article 3 (2) will also be included, but an in-depth analysis of the territorial scope will not be conducted due to the nature of the topic.

As an assessment leading up to an adequacy decision is very extensive and time consuming, and demanding a high level of expertise of which I do not hold, the thesis will be limited to an assessment of the possibility of an adequacy decision, not an attempt to conduct the actual adequacy assessment required by Article 45 of the GDPR. The thesis aims to present the legal criteria for adequacy decision and to present some important observations regarding the Chinese data protection framework in relation to these criteria, in order to consider the possibilities of an adoption of an adequacy decision.

The thesis is narrowed to sources available on and before 30 November 2019.

2. The GDPR

2.1 An introduction to the GDPR

The GDPR entered into force on the 25th of May 2018, replacing the Data Protection Directive 95/46. It provides one of the most extensive personal data protection laws in the world and makes up the core of the EU data protection legislation (also including the three EFTA states Norway, Iceland and Liechtenstein).[24] In order to safeguard that the level of protection guaranteed by the GDPR travels with the personal data when it is transferred outside of the EU, the GDPR also contains different mechanisms for safely transferring personal data to third countries. Chapter 5 of the GDPR contains the tools that can be used to execute third country transfers, including the legal basis of adequacy decisions.

The objectives of the GDPR are emphasized in Article 1, including the protection of the processing of natural persons' personal data and the free movement of personal data within the EU. In short, the GDPR seeks to implement a market permitting free flow of personal data while also providing safe and lawful processing where the data subjects´ personal data and other rights are adequately protected.[25]

2.2. The territorial scope of the GDPR

As the GDPR extends its territorial scope for specified processing activities, it is important to understand how and when the regulation is applicable for anyone outside the EU, including organizations based in China.

As previously stated, the GDPR contains a broader scope of application than that of Directive 95/46. There was made an effort to clarify the scope of application as the previous provision was vague and left room for confusion and misinterpretation. The GDPR clarifies the uncertainty regarding the scope of application to a large extent by including extraterritorial applicability.

---

[24] GDPR was incorporated into the EEA Agreement by the EEA Joint Committee on 6 July 2018 through the adoption of a Joint Committee Decision 154/2018 para. 10; The GDPR was incorporated into Norwegian law pursuant to Personopplysningsloven of 15 June 2018 number 38.
[25] GDPR Article 1

One reason behind the extended territorial scope is the fact that the GDPR was passed as a regulation, as opposed to a directive such as the previous data protection legislation. While the content of Directive 95/46 could be interpreted differently in the various member states due to its nature as a directive, the provisions of the GDPR are directly applicable in its entirety throughout the EU due to its position as a regulation.[26] One of the thoughts behind establishing the new provisions in a regulation was to diminish the national differences leading to legal uncertainty and lack of coherency throughout the Union under Directive 95/46. In fact, in the proposition of the GDPR it was emphasized that "the EU needs a more comprehensive and coherent policy on the fundamental right to personal data protection".[27]

The territorial scope of the GDPR appear in Article 3. The first paragraph sets out the standard territorial scope, stating that the GDPR is applicable for "processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union".[28] Paragraph two further broadens the territorial scope as it makes the GDPR applicable outside the EU territorial jurisdiction if specified criteria are met. The third being application to controllers located outside the EU where member state law is applicable by virtue of international law.[29] In connection with application for Chinese organizations, Article 3 (2) is the obvious legal basis, thus making this paragraph the focus in the following presentation.

2.2.1 The criteria of Article 3 (2)

Article 3 (2) sounds as follows:

> "2. This regulation applies to the processing of personal data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
> (b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

[26] TFEU Article 288
[27] COM/2012/011 final p. 2
[28] GDPR Article 3 (1)
[29] Ibid. Article 3 (3)

By way of introduction, it is worth to mention that the targeting criterion applies to all natural persons staying within the EU zone, regardless of their nationality or official place of residence.[30] For example, this means that the GDPR will be applicable to any Chinese based data controllers processing information or offering services to Chinese nationals as long as they are residing within the EU. The application of the GDPR cannot be avoided due to the fact that the personal data belongs to Chinese nationals, for example. This will also be the outcome regardless if the persons in question are staying within the EU short term i.e. on vacation or a business trip. Seen in correlation with Article 8 of the Charter of Fundamental Rights, this corresponds with the evident principle assuring the right of data protection to "anyone", not just EU citizens. The GDPR should be interpreted in accordance with the Charter due to its position as primary EU law.[31] The point of intersection of relevance will be the location of the individual(s) at the time when the relevant trigger activity takes place.[32]

Yet, the EDPB has stated that processing in itself is not sufficient in order for the GDPR to be applied if the controller or processer is established outside the EU. It is also required that the element of "targeting" persons within the EU must be present. As articulated in Article 3 (2) b), this element can be present either through the offering of goods or services, or through monitoring behavior.

An example of offering goods or services could be a Chinese based company selling products that are made available for sale within the EU, offering payment in currencies such as EURO and GBP, being available in EU languages such as English, French and German, offering shipping to European countries and so forth. A practical example of application through monitoring behavior would be when a Chinese based company has an app that processes location data of the costumers while specifically targeting the EU market.

This thesis will not complete a full assessment of these criteria as this is extensive and outside the scope of the thesis. The core of Article 3 (2) is that companies located within China or any other third country or territory, may be subject to the relevant provisions of the GDPR if they

[30] Confirmed by GDPR Recital 14
[31] Lenaerts and van Nuffel (2011), p. 831-832
[32] EDPB Guidelines 3/2018 p. 13

offer “goods or services” or “monitor behaviour”, targeted at data subjects located within the EU.

3. Adequacy decisions

An adequacy decision is an implementing act by the Commission which confirms that third countries, territories, specific sectors in third countries or organizations provide the same level of data protection as within the EU zone.[33] The effect of an adequacy decision is that personal data can flow freely between the EU and the third country or organization in question, without the need of any additional authorization.[34] This reduces the workload affiliated with third country transfers, by, among other things simplifying the regulatory environment for international business. However, these decisions do not however cover the exchange of data in the law enforcement sector, such as data governed by the so-called "Police Directive".[35]

The legal basis of adequacy decisions is the GDPR Article 45, stating that such a decision "may take place where the Commission has decided" that the country in question "ensures an adequate level of protection", see Article 45 (1). Paragraph 2 of Article 45 further specifies the elements the Commission shall take into consideration when assessing the adequacy level of the country or organization in question, hence what is needed to satisfy the criteria of "adequate level of protection" in Article 45.

To this date (December of 2019), the Commission has adopted adequacy decision with respect to Andorra[36], Argentina[37], the Faroe Islands[38], Guernsey[39], Israel[40], Isle of Man[41], Japan[42], Jersey[43], New Zealand[44], Switzerland[45] and Uruguay[46]. There are also acts in place on Canada[47]

[33] GDPR Article 45 (1)
[34] EC, "Adequacy decisions"
[35] Directive (EU) 2016/680 Article 36
[36] 2010/625/EU
[37] 2003/490/EC
[38] 2010/146/EU
[39] 2003/821/EC
[40] 2011/61/EU
[41] 2004/411/EC
[42] (EU) 2019/419
[43] 2008/393/EC
[44] 2013/65/EU
[45] 2000/517/EC
[46] 2012/484/EU
[47] 2002/2/EC

and the United States[48], although neither is of full value adequacy decisions. Both are limited to more precisely demarcated companies who meet given data protection criteria.[49]

3.1 Schrems v. Data Protection Commissioner

This concept of "adequate level of protection", which already existed under Directive 95/46, has been further developed by the CJEU. The current legal standard of the adequacy term was set by the CJEU in *Schrems v. Data Protection Commissioner.*[50] The judgement concerned a complaint by Maximilliam Schrems against the Irish Data Protection Commissioner, concerning the former adequacy decision on the US, called "Safe Harbor". He argued that the United States did not offer an adequate level of data protection in light of the revelations made by Edward Snowden in 2013, revealing that the United States did not offer adequate protection against surveillance by public authorities. According to Schrems, the transfer of personal data by Facebook Ireland to servers located in the United States for processing were consequently unlawful. The Irish Data Protection Commissioner rejected the complaint, whilst the Irish High Court heard the case, but decided to stay the proceedings and refer the case to the CJEU. The CJEU ultimately held that the Safe Harbor agreement enabling transfers of personal data between the EU and the United States was invalid. The judgement was based on the grounds that the agreement permitted public authorities to have access to personal data on a general basis, which undermined the fundamental right to respect for private life assured by the EU Charter Article 7. Based on this, the CJEU held that the decision did not offer an adequate level of protection as the Commission had failed to prove that "the United States in fact 'ensures' an adequacy level of protection by reason of its domestic law or its international commitments", as was required by Directive 95/46 Article 25(6).[51]

The CJEU went on to clarify the legal standard of data adequacy, stating that the level of protection in the third country had to be "essentially equivalent" to that guaranteed in the EU. Furthermore, the court stated that "the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within

[48] (EU) 2016/1250
[49] EC, "Adequacy decisions"
[50] *Schrems v. Data Protection Commissioner,* C-362/14
[51] Ibid. para. 97

the [EU]"[52]. Consequently, it was clarified that the personal data framework did not necessarily have to mirror the European legislation point by point, but an adequacy decision had to establish that the essential core requirements of the data protection legislation was adequate.[53]

3.2 The procedure for the adoption of an adequacy decision

The procedure to be followed in order to adopt an adequacy decision in accordance with Article 45 is a four-step process. It starts with a proposal from the Commission, followed by an opinion by the European Data Protection Board, and subsequently an approval from the EU countries' representatives. Finally, the decision has to be adopted by the Commission.[54]

Before an adequacy decision can be passed, a comprehensive assessment of the adequacy level is required. This includes an evaluation of the legislation in place to protect the personal data and regulate the data processing, the extent of oversight mechanisms as well as the level of compliance and implementation in practice.[55] In addition, the assessment includes a review of the limitations and protection that are applied in order for personal data to become available to local and government authorities.[56]

At any point in this process, the European Parliament or the Council may request an amendment or withdrawal of the adequacy decision on the basis that it exceeds the implementing powers provided by the GDPR. The Commission has a duty to "repeal, amend or suspend the decision" see the GDPR 45 (5). The EDPB also has a supervisory function in relation to the adequacy assessment. One of the relevant tasks is to provide an opinion to the Commission "assessing whether a third country, a territory or one or more specified sectors within that third country; or an international organisation no longer ensures an adequate level of protection".[57]
The CJEU can also review this process and stop it at any time. This power is not limited to the time leading up to the adoption of an adequacy decision, but also extends to the time after a decision has been implemented. An example is when the CJEU found the former data transfer agreement between the EU and the United States Safe Harbor invalid in the judgement of

[52] *Schrems v. Data Protection Commissioner*, C-362/14, paras. 73 and 74
[53] WP 254 rev.01 Chapter 1
[54] Ibid.
[55] Ibid.
[56] GDPR Article 45 (2) (b)
[57] Ibid. Article 70 (1) (s)

Schrems v. Data Protection Commissioner.[58] As mentioned in the previous section, the CJEU found that the Safe Harbor decision failed to "comply with the requirements laid down in Article 25(6) of Directive 95/46".[59] This action was taken 15 years after the introduction of the Safe Harbor Agreement.

Once an adequacy decision has been passed and implemented, the effect is that personal data can be transferred to the third country, sector or organization as if the data was transferred within the EU. Adequacy decisions will however not be upheld indefinitely. They are to be subject to a "periodic review, at least every four years".[60] The decisions need to be closely monitored as there might occur developments which will affect the level of protection ensured in the third country.[61] Specific incidents or special arrangements may require reviews at a more rapid rate than the main rule of four years. An example of this is the Privacy Shield agreement with the United States which is subject to annual review.[62]

3.2.1 The legal criteria

The following paragraph contains a closer look at the legal criteria that needs to be met in order to bring about an adequacy decision. The legal basis, Article 45 (1) and (2) of the GDPR sounds as follows:

> "1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.
> 2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
> (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and

[58] *Schrems v. Data Protection Commissioner*, C-362/14, para. 52
[59] Ibid., para. 98
[60] GDPR Article 45 (3)
[61] Ibid. Article 45 (3) and (4)
[62] (EU) 2016/1250 para. 52

security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the date subjects in exercising their rights and for cooperating with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data."

Summarized; an adequacy decision may only find place when there is "an adequate level of protection" in accordance with paragraph 1. The Commission shall particularly take into consideration three key elements; (a) the state of data protection law in the country, including how it is enforced and redress of data subjects, (b) whether there are functioning and independent supervisory authorities responsible for the compliance of the legislation mentioned in (a), and (c) international commitments or other legally binding obligations. The assessment is virtually a two-step assessment: it requires an analysis of the content of rules that are applicable within the country in question, as well as the means in place to ensure an effective application of these rules.

The Commission has also found that the extent of the EU's commercial relationship with the country, the extent of personal data flow to the country, the pioneering role the third country plays in this field and the overall political relationship with the country shall be taking into consideration while conduction an adequacy assessment.[63]

[63] EC MEMO/17/15

In order for data adequacy to exist with a third country, complete resemblance to the EU rules or system is not required. In accordance with the CJEU's judgement in *Schrems v. Data Protection Commissioner*, the level of protection ensured for personal data in the country in question must be "essentially equivalent".[64] The adequacy assessment includes several different factors that are tailored against an overall assessment of each individual case.

3.2.2 The procedure used in the adequacy decision with Japan

The adequacy decision on Japan was adopted on 23rd of January 2019, resulting in the creation of the largest area of safe data flow in the world.[65] Alongside the adequacy decision adopted by the Commission, a corresponding decision was adopted in Japan.[66] President Juncker of the Commission and Prime Minister Abe of Japan publicly committed to adopting an adequacy decision as early as in July of 2017.[67] The talks were concluded roughly one year later.[68] What makes the decision on Japan important, is that this was the first adequacy decision to be adopted after the implementation of the GDPR. It correspondingly sets a standard for how future adequacy assessments will be conducted.

To start the procedure, the Commission developed a draft Decision, which both The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) and the EDPB gave their response on. The resolution adopted by LIBE contained several criticisms of the draft decision.[69] The criticism consisted of twelve main points. It included the lack of sufficient clarification regarding the type of EU personal data covered by the adequacy decision, the independence of the Personal Information Protection Commission of Japan (PPC), insufficient levels of fines, the opportunity for business operators to voluntarily hand over data to law enforcement, and Japanese mass surveillance.[70] Shortly summarized, LIBE did not find that the draft had proven data adequacy in Japan.

---

[64] *Schrems v. Data Protection Commissioner*, C-362/14, paras. 73 and 74
[65] (EU) 2019/419
[66] EC Press Release (2019)
[67] EC Statement (2017)
[68] EC Press Release (2018)
[69] EP Resolution (2018); Greenleaf (2019) p. 9
[70] Graham (2018), "Japan and Korea: Different paths to EU adequacy"

The EDPB gave an Opinion on the draft decision following a plenary session in December 2018. This opinion also contained criticism of the draft for not proving adequacy.[71] It was also expressed that as this was the first adequacy decision to be adopted after the GDPR came into force, the decisions would be "of paramount importance [because] it will set a precedent".[72] Meaning the EDPB acknowledged how the procedure and content of this decision would be used as a reference in any future adequacy assessment.

As a part of the work to conclude an adequacy decision, Japan agreed to revise and update its data protection laws in order to meet the comprehensive rules set forward by the GDPR. This was proven necessary based on the feedback given by LIBE and EDPB. These updates included implementing stricter provisions for re-transferring personal data that originated from the EU, stricter provisions for processing of sensitive data and enabled a new mechanism allowing EU citizens to file complaints against the Japanese data protection authorities if their personal data is unlawfully processed. These changes all went into effect as the adequacy decision was adopted.[73]

This past subsection aims to create a picture of the adequacy decision process, but also to illustrate how the adoption of an adequacy decision is a step-by-step procedure which develops over time. The third country is not required to have "essentially equivalent" data protection frameworks once talks concerning adequacy decisions have started. This is the level of adequacy required by the conclusion of the process.

[71] EDPR 5th Plenary Session
[72] Ibid.
[73] EC Press Release (2019)

4. Data Adequacy and China

This section will provide a review of the Chinese data protection framework compared to some of the important elements of the GDPR. The segment will take a look at some of the main differences and similarities of the two frameworks and attempt to evaluate the consequences this will have for the possibility of a future adequacy decision.

4.1 An introduction to Chinese data protection law

Data protection law in China is a relatively new concept compared to most EU countries. As with many concepts in China, the field of data protection law has been subject to a rapid development, unlike the EU, where the development has come about gradually over a longer period of time. Prior to the implementation of the CSL in June of 2017, there was in fact no data protection law in China. The different provisions that did exist were scattered around in different laws and regulations, and mostly focused on system and infrastructure security as opposed to personal data.

The drafting of the CSL started in 2015, and the need for personal data protection legislation became evident soon after. During the summer of 2016, two students died in a matter of days due to heart attacks as a result of their personal data being misused to commit fraud, causing them to lose their tuition money. Their deaths sparked public outrage and showed a dangerous downside for the lack of personal data protection legislation in China. In the wake of these events and the need to keep up with the global development of the field, the CSL was adopted and came into effect roughly a year later.[74]

The data protection framework in China still consist of a complex framework with several laws and regulations, in addition to many different governmental administrators and committees.[75] With the vast amount of regulations and involved institutions, the system can be difficult to follow at times. This poses a threat to the legal certainty or so-called predictability of the organizations subject to the data protection framework.

[74] China Daily, "Student suffers fatal cardiac arrest after telephone scam"; China.org.cn. "Telecom fraud claims life of another student"
[75] Triolo and others (2017)

4.1.1 The Chinese Cybersecurity Law

The CSL is a comprehensive piece of legislation. In addition to regulating the protection of personal data and restricting the onwards transfer, it also includes penalties such as the suspension of business activities, fines and the revocation of licensing and other sanctions for neglecting to accommodate to the provisions.[76] Consequently, it is not a pure personal data protection regulation in the sense of the GDPR. Chapter 4, which is titled "Network Information Security" focuses on protecting personal data and will correspondingly be the most relevant section in regard to the adequacy assessment. It is worth to mention that CSL only applies to "network operators". This term is commonly used for organizations providing network services in digital form. Thus, will the protection of the CSL only extend to the personal data of network users.[77] Personal data stored in any non-digital item such as for example paper, will not be protected under this law.[78]

4.1.2 The Standard

The Standard[79] was issued in of December 2017 by the Standardization Administration of the People's Republic of China (SAC), coming into effect just a couple of weeks before the GDPR in May 2018. The development of the Standard came as a result of joint work by the government, industries as well as academics. It sets out a full set of voluntary guidelines relating to the processing of personal data. Although it is not a legally binding regulation, it is a respected national standard under the system of the CSL. Its legal status can be compared to soft law within the EU.

As previously stated, the Standard is not legally binding, meaning it cannot be legally enforced. This weakens its legal position and influence in relation to the adequacy assessment. Despite this, the Chinese government has since its release used it as a reference to point at shortcomings and data protection issues in several big companies who were not in compliance with its guidelines. This shows that despite its voluntary nature the Standard has legal force through the application by Cyberspace Administration of China (CAC).

---

[76] See CSL Articles 61 and 66
[77] Ibid. Articles 40 - 50
[78] Han and Munir (2019) p. 535
[79] Information Technology – Personal Information Security Specification, BG/T 35273-2017

For example, in January 2018 Ant Financial was criticized after it became evident that the company automatically enrolled users of their services to a credit scoring by a third party after paying on the website. In response to the public outrage, the CAC interviewed both Ant Financial and the third part Sesame Credit.[80] An interview meaning a summoning by the relevant authority to converse and point out serious violations of laws and regulations and issue orders of rectification and correction. This shows that even though the Standard has limited legal impact in theory, it is still used to hold companies accountable and make them comply with its norms.[81]

Two other major companies, Baidu and Beijing ByteDance Technology have also been reprimanded for not informing their users that their personal data was used and how it was processed. Three additional companies were given instruction to immediately improve and correct their privacy policy in order to protect their users' personal data privacy rights and interests. If these companies failed to correct, they would face administrative punishment.[82] This further legitimizes the provisions of the Standard through the enforcement by CAC.

The above-mentioned examples show that the Standard and its provisions have been enforced by CAC regardless of its voluntary nature. It is also clear that organizations following the guidelines of the Standard will gain credibility amongst its customers and the general public because it shows that the company is taking data protection issues seriously. This gives a stronger incentive to implement these provisions, even if they are not legally obliged to do so.

Together with the CSL, the Standard constitutes the core of the Chinese data protection framework, and thus will be used in the following assessment.

4.2 How the Chinese framework measures to the GDPR

The WP 29 has summarized some key content principles that need to exist in a third country in order to have an adequate level of protection. In the following, the Chinese framework will be

[80] An affiliate of Alibaba Group and the highest valued FinTech company in the world. It has 588 million users of its mobile payment network 'Alipay'.
[81] Han and Munis (2019) p. 536;
Chin, Josh, "Chinese regulator rebukes Ant Financial for automatic credit scoring enrollment"
[82] Han and Munir (2018) p. 536

held up against some of these principles. This section will highlight some of the similarities and differences of the Chinese framework and the GDPR and take a look at observations that would be taken into consideration by the Commission in an adequacy assessment.[83]

By way of introduction, there are several evident similarities between the Chinese framework and the GDPR. They both aim for purpose limitation, data minimization, transparency, security, confidentiality and integrity in data processing, as well as both containing accountability principles for controllers.[84] In addition, the scope of application of both the GDPR and the Standard covers both the private and the public sector.[85] Such similarities lay the foundation for further work towards an adequacy decision.

4.2.1 Concepts

Basic concepts of data protection not necessarily mirroring, but at least consistent with the concepts of the GDPR are required for a country to have an adequate level of protection. As mentioned in subsection 1.4; concepts corresponding to "personal data", "processing" and "controller" are found in the Chinese framework. The term "processor" and "recipient" are not defined, but without being conclusive in regard to the adequacy assessment as mentioned in subsections 1.4.4 and 1.4.5. The term "sensitive data" does however require some further clarification.[86]

The Standard operates with the term "Personal Sensitive Information", which presumes to be in concurrence with "special categories of personal data" in the GDPR[87] For future reference, the term "sensitive data" will be used as this is utilized by WP29. The scope of sensitive information in the Standard seems to be more far-reaching than the corresponding term of the GDPR Article 9 (1). In addition to racial origin, generic data, biometric data, health data and data regarding one's sexual orientation, which is also included in the GDPR, the Standard includes identity card number, bank account number, telephone number, email address, geo-locations and more in its definition. It would be almost impossible to list all the examples of

[83] WP 254rev.01 Chapter 3
[84] CSL Articles 40, 41, 42 and 43; The Standard Article 4
[85] GDPR Article 2; the Standard Article 1
[86] WP 254rev.01 Chapter 3
[87] GDPR Article 9

what might be counted as sensitive information, the Standard has included a broad and non-exhaustive list, including six categories and over fifty examples.

In addition, any personal data about a person under the age of 14 is also rendered as sensitive data in the Chinese system.[88] In fact, new provisions dedicated to protecting children's personal data came into effect in China on 1st of October 2019. It only governs storage within China, but contains strict provisions regarding consent and restricted internal access to this type of data, these guidelines represent an effort to strengthen the protection of sensitive personal data.[89] The GDPR on the other hand, requires guardians to consent to processing of personal data of children under the age of 16, but does not automatically consider this sensitive data.[90]

This indicates that we find many of the basic data protection concepts of the GDPR in the Chinese framework. They are not identical, which this is not required as long as they are somewhat consistent with those of EU law. As to the fact that sensitive data is defined much wider in China indicates that the concepts are not consistent with the concepts of the GDPR. On the other hand, the more far- reaching scope makes it harder for organizations to evade the special requirements applied to the processing of sensitive data. Consequently, the Chinese framework help ensure better data protection when it comes to processing their sensitive data. This complies with the objective of the GDPR to protect the personal data of natural persons in Article 1.

4.2.2 Grounds for lawful processing

The CSL enables processing of personal data when the data subject has consented, meaning processing without consent to be unlawful.[91] The GDPR on the other hand presents six alternative grounds for lawful processing, consent being only one of them. The remaining grounds being processing necessary for the performance of a contract, compliance with legal obligation, protection of vital interests, public interest or legitimate interests.[92] These alternative grounds are included in the GDPR as the requirements for consent will sometimes not be possible to fulfill. Article 7 of the GDPR requires consent to be demonstrated, the consent

[88] The Standard Article 3 (2)
[89] Provisions on Cyber Protection of Children´s Personal Information
[90] GDPR Article 8
[91] The Standard Article 5 (3)
[92] GDPR Article 6 (1) (b) - (f)

request to be given in a distinguishable context, the possibility to withdraw the consent and that the consent is not given as a condition for performance of a contract where the processing is not necessary.[93] The essence of this provision is that consent must be given freely which can only occur if the data subject has a genuine choice on whether or not to consent and is fully informed about what he or she is consenting to. The reasoning behind this is to protect data subjects from being coerced into consenting to processing due to external factors. With consent being the only lawful form of processing in the Chinese framework, this may pose a problem in relation to the adequacy assessment seeing as these considerations are not addressed.

Furthermore, the Chinese framework operates with two different types of concept, explicit and implied. Specified provision in the Standard requires explicit consent by the date subject, including processing of sensitive data. Antithetical, this indicates that remaining provisions without this specification only requires implied consent in order to be lawful. The concept of implied consent does not exist in the GDPR.

The problem with implied consent is that it can be hard to prove that consent is given and that the data subject was fully aware of what him/her was consenting to. This further provides companies with a margin for stretching consent when it hasn't necessarily been given or when the data subject has not properly understood what he/she has consented to. Allowing implied consent as a legal basis for data processing is undermines the data processors' rights by not allowing them a legitimate choice for consent. Accordingly do the Standard not offer the same level of protection as the GDPR in relation to consent. This indicates that the grounds for lawful processing in the Chinese framework are not essentially equivalent to that of the GDPR. [94]

A similarity is that both the GDPR and the Standard permits processing of personal data with exceptions from the provisions of lawful purpose for processing. The GDPR Article 23 enables such processing in cases where it is necessary to safeguard the national security and defense, necessary in the public interest, compliance with legal obligations, to protect the vital interest of the data subject or another person, or if it is necessary for the performance of a contract which the data subject is part. The Standard enables processing without consent when this is

[93] GDPR Article 7
[94] WP 254rev.01 Chapter 3

necessary in order to fulfill a contract and directly related to national security or defense, among other things.[95]

4.2.3 The right of access, rectification, erasure and objection

Other important principles like the right of access, rectification, erasure and objection are important to establish in the Chinese framework in order for an adequacy decision to be a possibility.[96] The Standard assures data subject's right to rectification and erasure in accordance with Articles 7.5 and 7.6. Although the right to objection is not explicitly mentioned, there are provisions requiring data controllers to offer means for data subjects to lodge complaints, as well as to respond to these within reasonable time, see Articles 7.10 and 7.12. This indicates that the right of objection is also present in the Chinese framework.

When it comes to the right of access, Article 7 (4) and 7 (9) of the Standard require controllers to provide access and copies of specified categories of personal data upon the data subjects request. Copies are to be provided of "basic information and information about their identities" as well as "health, psychological, educational and work information".[97] In accordance with the GDPR, the right of data subject to request copies of all personal data processed is a key principle, making restricted access in accordance with the Chinese framework problematic in relation to a possible adequacy decision. A practical example of this right being asking a social media provider where you have a profile for a copy of the personal data they have stored about you.[98]

4.2.4 Restrictions on onward transfers

Another essential element to be assessed is onwards transfers of personal data.[99] In order to be "essentially equivalent"[100] the Chinese framework need to contain restrictions on when personal data may be transferred onwards, both for domestic transfers to third parties and transnational transfers. The essential elements required are that the recipient of the onward transfer must offer

[95] The Standard Article 5 (4)
[96] GDPR Articles 12, 15, 16, 17 and 21
[97] The Standard Article 7.9
[98] WP 254rev.01 Chapter 3
[99] Ibid.
[100] *Schrems v. Data Protection Commissioner,* C-362/14, paras. 73 and 74

an adequate level of protection. This is a must in order to ensure that the data protection level won't be undermined by the transfer and that there is a legal ground for the transfer.
For domestic transfers, the Standard requires Chinese controllers to conduct a security impact assessment in order to assure the safeguard of the personal data to be transferred. As previously mentioned, the Chinese framework does not define a processer, and neither does it define a "third party" as the GDPR does in Article 4 (10). The same considerations should be asserted to the relationship between third parties as with the relationship between controllers and processors; the controllers have the ultimate responsibility in accordance with the Chinese framework and will have to take responsibility for safeguarding any transfers of personal data. So, in order to transfer personal data, Chinese controllers are required to perform a security impact assessment, leaving it up to them to decide if the protection offered is sufficient, and intimately having to bear the consequences if this turns out to be incorrect.

For transfers outside of the EU, the European framework requires the initial recipient, that being the one transferring the personal data onwards, to be responsible for the safeguarding of the transfer in the absence of an adequacy decision. Other safeguards can be factors such as a legally binding and enforceable instruments, binding corporate rules or contractual clauses etc. that assures the data protection of natural persons are not undermined. In specified cases, such transfers also require authorization by the competent supervisory authority.[101] In other words – the GDPR contains strict rules regarding the transfer of personal data outside of the EU.

As already mentioned, the transfer of personal data outside of the EU in accordance with the GDPR depends on the level of data adequacy in the recipient country. Thus, it be evaluated how the Chinese framework regulates transnational transfers of personal data.

The legal basis for transnational transfers is either the CSL Article 37 and the Standard Article 8.7. The CSL only applies to "critical information infrastructure operators" that "produce personal information or important data"[102], meaning that these transfer requirements are not applicable to all Chinese data controllers. The main rule in accordance with the CSL is that the personal data is to be stored within China, with exceptions of when transfers out of the country

[101] GDPR Article 46
[102] CSL Article 37

are “truly necessary” “due to business requirements”.[103] In any case, a security assessment is required, in addition to compliance with any relevant laws or regulations that may apply.

The Standard Article 8.7 has broadened the scope of application to all “network operators”. Equivalent to that of the CSL Article 37, this provision also requires a security assessment and compliance with relevant regulations and provisions. The Standard does however not clarify the closer criteria of what this assessment consists of. The CAC has released a revised draft of “Personal Information Outbound Transfer Security Assessment Measures” (the Measures) the latest draft issued in June 2019. It aims to clarify the requirements of such security assessments. The main elements of these provisions are that organizations are to present transfer security assessments to the provincial-level cybersecurity and informatization department.[104] This assessment shall contain a declaration form, the contract entered into between the operator and the recipient, an analysis report on the security risk associated with the transfer, as well as other materials that will be required by national cybersecurity and informatization departments.[105] This shows that in many instances, a self-assessment consisting of said criteria will suffice to conduct a security assessment for transnational transfers in accordance with the Chinese framework. The Measures do however contain a provision enabling the relevant cyberspace and informatization department to terminate transnational transfers if:

> “1. Network operators or recipients experience incidents or relatively serious data breach or abuse;
> 2. It is impossible or difficult for the data subjects of the personal information to defend their legitimate rights or interests;
> 3. The network operators or recipients are incapable of safeguarding the security of personal information.”[106]

The above-mentioned provisions show that the main rule is that transnational transfers can be conducted in accordance with the Chinese framework when a security assessment has been conducted. Exceptions are made in instances mentioned above, where CAC has the authority to terminate the transfers. In accordance with the Chinese framework, controllers seem to have

[103] Ibid.
[104] The Measures Article 3
[105] Ibid. Article 4
[106] Ibid. Article 11

more responsibility affiliated with evaluating the protection provided by third parties. This includes conducting the security impact assessment and making sure that appropriate safeguards are in place before a transfer can take place. As opposed to the GDPR where there are more stringent requirements that need to be met in order for a lawful transfer out of the EU. However, the Measures regarding cross-border transfers helps elucidate how transnational transfers are regulated in China, but it is conceivable that more stringent conditions for such transfers would be necessary in order to reach an adequacy decision. Companies can more easily emphasize self-interests and profit when they conduct the impact assessments themselves, which would undermine the data subjects' rights.

4.2.5 Specific safeguards for special categories of data

An additional element of significance is whether the Chinese framework offers specific safeguards for special categories of data, focusing on sensitive data in particular. The term "sensitive data" has already been defined in subsection 4.2.1, as it has been established that the term also covers what is referred to as "personal sensitive information" in the Chinese framework.[107]

The GDPR Article 9 (1) establishes a main rule where processing of sensitive data is prohibited. Paragraph 2 further presents ten exceptions where processing may still find place, including (a) implicit consent by the data subject, (b) where the processing is necessary in order to carry out certain obligations, (c) to protect the vital interest of the data subject or another natural person, (i) and (j) for reasons of public interest and more. The list presented is exhaustive, meaning that all sensitive data not included in these definitions are prohibited to process.[108] The essence is that for the Chinese framework to be essentially equivalent, special grounds of lawful processing of sensitive data are required. The grounds should be more stringent than those for processing regular personal data in order to better assure their safeguarding.

The Standard requires explicit consent when processing sensitive data.[109] Implied consent is as previously mentioned accepted in accordance with some of the Chinese provisions but will not

[107] WP 254rev.01 Chapter 3
[108] GDPR Article 9 (1) (a) - (i) for complete list.
[109] Consent given "through a written statement or an affirmative action on the PI subject's [data subject's] own imitative", see The Standard Article 3.6

suffice as a legal ground for processing sensitive data. In addition, a controller should inform the data subject of the functions of the sensitive data collection and explain the impact a refusal of consent will have. Special requirements are also imposed on the processing of sensitive data regarding a child, including the requirement of explicit consent by a guardian for any child below the age of 14.[110]

The fact that the Standard contains specific requirements for processing of sensitive data is good news when it comes to the possibility of an adequacy decision. This category of personal data is especially protected by the GDPR, and thus these rights must also be guaranteed an adequate level of protection in any third country where an adequacy decision is to be considered. Seen in relation with the fact that the Chinse framework through the Standard contains a very broad definition of sensitive data (see subsection 4.2.1). This indicates that the level of protection of sensitive data in China may even be stronger than that of the GDPR.

4.2.6 Obligations in case of security breaches

Another characteristic of interest when assessing the adequacy level is the difference in obligations arising from the two different frameworks regarding security breaches. According to the provisions of the CLS, network operators are required to notify both network users and report to the competent authorities as soon as possible after a breach has occurred or potentially will. The Standard helps provide more in-depth provisions regarding the obligations network operators are submitted to. This includes requirements to formulate response plans in regard to possible security breaches in the future, and no less than annual response training for staff. In the event of a breach a controller is also required to record relevant information, including the amount of effected information, individuals etc.[111]

Data controllers subjected to the GDPR shall "without undue delay" notify the competent supervisory authority and communicate to the affected data subjects in the event of a data breach.[112] In the event of a personal data breach the Standard also asks controllers to report

[110] The Standard Article 5.5 a), b) and c)
[111] Ibid. Article 9.1
[112] GDPR Articles 33 (1) and 34 (1)

these elements to the relevant authority and subjects, correspondingly to reaction required by the GDPR.[113]

One issue in the Chinese framework is that it is not specified which exact authorities to report to. The CSL Article 42 states that in the event of a "leak, destruction, or loss of personal information", network operators are to "make a report to the competent departments in accordance with regulations". The CLS does however not specify how to identify the competent authorities, leaving it uncertain for operators where to report. This is in contrast to the GDPR which specifies that breaches should be notified "to the supervisory authority competent in accordance with Article 55".[114] Article 55 contains the legal basis for national supervisory authorities, indicating that reports are to be made to the national supervision authority in the relevant Member State.

In 2017 CAC released a supporting regulation named "the National Cybersecurity Incident Response Plan" (the Plan). It aims to clarify which authorities within China the breaches are to be reported to. In the Plan, data breaches, which is referred to as incidents, are divided into the four sub-categories: general, relatively significant, significant and extraordinarily significant, from the least to the most serious. The contents of this plan will not be examined closely, but what is relevant relating to this question, is the fact that it puts CAC in charge of coordinating other relevant government authorities regarding the handling of what they call "Cybersecurity Incidents", meaning data breaches. In addition, the translations of the Plan point out that the authorities are to be divided into specific sectors as well as geographical jurisdictions, where they will be responsible to handle data breaches within this jurisdiction.[115]

Recent procedure has also shown that the CAC has taken the main role of enforcing the CSL and data protection laws in China in general. The content of the Plan seems to support this notion of the CAC as a senior authority regarding supervision and enforcement of the Chinese data protection framework. See subsection 4.1.2 for such examples.[116]

---

[113] The Standard Articles 9.1 and 9.2
[114] GDPR Article 33 (1)
[115] CMS, "China publishes the National Cybersecurity Incident Response Plan"
[116] WP 254rev.01 Chapter 3

4.2.7 Appointment of Data Protection Officer

In short, a Data Protection Officer (DPO) is someone who oversees a company's data protection strategy and GDPR compliance.[117] The GDPR requires the appointment of a DPO in any case where (a) processing is carried out by a public authority, (b) the core activity of a controller or processor requires a regular and systematic monitoring on a large scale or (c) when the core activities of the controller processor consist of processing a large scale of special categories of data [sensitive data].[118]

In accordance with condition (b) and (c), the appointment of a DPO is based on whether the organization process a "large scale" of data, not the size of the organization itself. There are however no provisions providing a more specific number or guidelines clarifying when processing is said to be considered at a large scale. Even the relevant guidelines for data protection officers released by the WP 29 is unable to give a concrete number for when this requirement was met.[119]

The Standard on the other hand, presents precise numbers for when Chinese companies are required to appoint DPO's. This includes when "the number of employees exceeds 200" or when personal data "of more than 500,000 people" is processed or expected to be processed within 12 months.[120] The Chinese framework seems to make it easier to companies to comply as they are given concrete numbers to relate to, while the GDPR is more flexible in its appointment of a DPO with a term that can be dynamic and develop with time.

Also, as evident in the GDPR Article 37 (1) (a), a DPO appointment is required when the processing is to be carried out by a "public authority or body" in accordance with the GDPR Article 37 (1). This is essential to prevent abuse of power and to assure effective protection against surveillance by public authorities. A corresponding provision is not found in the Chinese framework, which is a problem in connection to an adequacy assessment as this makes it easier for public authorities to access personal data, depriving data subjects of additional protection that an appointment of a DPO constitutes.

---

[117] GDPR Recital 97
[118] Ibid. Article 37 (1)
[119] WP 243 rev.01, para. 3.2.1
[120] The Standard Art. 10.1 c)

4.2.8 Summary

Even with the differences found in the Chinese framework, there are a lot of similarities indicating that the adoption of an adequacy decision may very well be a tangible possibility. Especially as at seems as if the Standard is mirrored after the GDPR to a large extent. It is interesting to see that some of the differences that presents themselves show that some of the provisions of the Standard presents stricter requirements than that of the GDPR, especially as Europeans tend to have a conception of their data protection laws being the strictest and most extensive.

Looking at the Japanese decision, the framework present in Japan at the time leading up to the adoption was not deemed to be adequate. They implemented changes to their data protection legislation as the adequacy decision went into effect, to make sure their frameworks were harmonized. This could also be a possibility for China if it was found that there were still shortcomings to their data protection framework after a proper adequacy assessment and process.[121]

[121] WP 254 rev.01

5. Enforcement and compliance mechanisms

In addition to having a legal framework which ensures a level of adequate protection, there are requirements regarding the enforcement and compliance mechanisms that need to be in place in order for a third country to offer an adequate level of protection. in accordance with the GDPR Article 45 and the other criteria mentioned in subsection 3.2.1. These mechanisms make up the second half of the adequacy assessment. This section will provide a brief review of the relevant elements with respect to the Chinese framework, followed by additional elements of relevance.

5.1 Supervision, compliance and accountability

The GDPR does not only require the existence of independent supervisory authorities, but furthermore that they are "effective functioning".[122] Meaning that their mere existence is not sufficient to meet the requirements, they must perform their tasks by providing a fair and legitimate implementation.

As the Standard is a voluntary Standard, it cannot be enforced in the same sense as the GDPR can. It is hard to carry out supervision activities for a set of guidelines that are not compulsory. The CSL does however contain provision regarding supervision, with Article 8 stating that different state departments are to plan and coordinate "cybersecurity efforts and related supervision and management efforts". Regardless, most of the relevant provisions that make the Chinese framework harmonize with the GDPR, are found in the Standard. It will therefore be decisive in an adequacy assessment whether or not the existence of supervision authorities who can enforce the provisions of the Standard exist.

Although CAC has shown that it will reprimand companies not in compliance with the provisions of the Standard, the supervisory system is not legally established or consistent in the sense of the EU system. On one hand, this indicates that China has a long way to go regarding data protection supervision. On the other hand, the practice of CAC display that the Chinese system in its own way has found a way to conduct supervision. It seems that lack of compliance to the Standard can be reprimanded in accordance with the requirement to adopt measures and

[122] GDPR Article 45 (2) (b)

other necessary measures in order to safeguard cybersecurity/personal data in the CSL Article 10.[123]

It's difficult to ensure compliance and accountability when there is a lack of a system to ensure properly functioning supervision. The Chinese framework has been known to contain many different institutions all having different responsibilities in regard to supervision and organization. A very complex data protection system can be difficult f to follow for both data controllers and subjects. The system does however seem to be getting better established, with CAC taking the leading supervision role and organizing subordinate institutions. A continued development in this direction is promising in relation to a possible future adequacy assessment.

A complicated matter is however that GDPR Article 45 (2) (b) also requires the supervisory authorities to be "independent". This is further specified in Article 52 stating for one that they "shall act with complete independence in performing its tasks" and also "remain free from external influence"[124]. Without conducting an in-depth deliberation on this section, it is a problem that the CAC conducts audits ('interviews'), gives punishment and other supervisory activity as it reports to the "Central Cyberspace Affairs Commission", which is headed by the Communist Party General Secretary Xi Jinping himself. The CAC will accordantly not pass the independence-test presented in the GDPR.

5.2 Additional elements

In addition to the criteria set out in Article 45, the Communication[125] has set out four additional elements to take into consideration during an adequacy assessment, as briefly mentioned in section 3.2.1.

5.2.1 Commercial relationship

First of all, "the extent of the EU's (actual or potential) commercial relationship with a given third country, including the existence of a free trade agreement or ongoing negotiations"[126] should be emphasized. As for China, it has already touched in on the fact that it is the EU's

[123]Zhang and Yin (2019)
[124] Ibid. Article 52 (1) and (2)
[125] The Directorate-General for Communication (the Communication) is the Commissions departments responsible for explaining EU policies to outside audiences.
[126] EC MEMO/17/15

second largest trading partner with daily trade estimated to be 1 billion EURO, see section 1.2.2. Currently negotiating a comprehensive investment agreement aiming to replace the individual investment treaties between China and member states. The next round of negotiations is to take place in Brussels in the week of 16th of December this year.[127] This showcase a strong commercial relationship which indicated a need for a safe and efficient way of transferring personal data, such as an adequacy decision.

5.2.2 The extent of personal data flows

The Communication further states that "the extent of personal data flows from the EU, reflecting geographical and/or cultural ties" shall be attributed importance.[128] There are no prominent geographical or cultural ties. Due to the amount of trade between China and EU and the big tech industry in China, it is however presumed that large flows of personal data are exchanged. The significance of a large amount of personal data exchanged is, as mentioned in the beginning of the thesis, indicates that an act on data adequacy would be valuable as it would facilitate the workload associated with transfers to third countries, promoting easier trade and cooperation.

5.2.3 China's role in the field of privacy and data protection

The "pioneering role the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region" should also be assessed, and in the case of the country holding such a pioneering role, this should be an incentive to work towards an adequacy decision.[129]

It is known that China does not have a good reputation internationally when it comes to privacy and data protection. There are constant talks about the government's mass surveillance such as the newly implemented social credit system. In addition, the tendency seems to be that public authorities can circumvent any data protection provision in the name of national security. Some examples will be provided below.

[127] EC, "Overview of FTA and Other Trade Negotiations"
[128] EC MEMO/17/15
[129] EC MEMO/17/15

First of all, the National Intelligence Law of 2017 has led to concerns globally as it forces Chinese companies to hand over personal data to the Chinese government. Article 7 states that "all organizations and citizens shall support, assist, and cooperate with national intelligence efforts". The Article has been criticized as it among other things encourage citizens to spy on each other.

What is to be regarded as "national intelligence efforts" is not clearly defined, and it seems to be a term the government choose to interpret as it please. A major problem with this law is that regardless of the legal framework and additional safety measures implemented in order to ensure adequate protection while transferring to China, a company can still be forced into sharing this personal data with the government on the pretense that it is necessary for national security efforts. This has for example been a major concern in relation to the implantation of Huawei's 5G network, resulting in countries such as the United States and Australia to block the company´s involvement in 5G networks. The concerns are that Huawei may be used to spy on data subjects pursuant to the National Security Law, making it a security risk to enter into contract with the company regardless of the undertaken safeguards. There has yet to be an EU decision on the matter, but a joint risk assessment report of 5G network security was released as late as in October this year. The report was developed by the Member States and with support from the Commission and the European Agency for Cybersecurity.[130]

In addition, a new set of guidelines referred to as MLPS 2.0 is to go into effect in China by the end of 2019. It includes three new guidelines that has sparked concerns internationally as it seems to be applicable to foreign owned companies operating in China and all data saved on servers within China.[131] One of the more important consequences of these new guidelines is that trade secrets will be subject to their application. Any "secrets" can automatically become available to the Chinese government, including government owned competitors and even the Chinese military.[132]

The CSL also includes a similar provision, requiring "any person or organization using networks […] must not use the internet to engage in activities endangering national security,

[130] EC, "EU-wide coordinated risk assessment of 5G networks security"
[131] BG/T 22239 – 2019; BG/T 25070 – 2019; BG/T 28448 – 2019
[132] China Law Blog, "China´s New Cybersecurity Program: NO place left to hide"

national honor, and national interests;".[133] It is presumed that to withhold personal data upon public authorities request could statute a breach of this duty.

Such provisions are problematic as they can be used by the public authorities to circumvent data protection provision and accordingly undermining the rights of data subjects. It also showcases that public authorities are not held to the same standard as organizations when it comes to data protection compliance. In accordance with GDPR Article 45 (1) a), whether public authorities have access to personal data is an element of the adequacy decision. The fact that this was essential for an adequacy decision became apparent in *Schrems v. Data Protection Commissioner*. This is essential for the effective safeguard of personal data and consequently data adequacy.

5.2.4 The overall political relationship with China

Lastly, "the overall political relationship with the third country in question, in particular with respect to the promotion of common values and shared objectives at international level" should be included in the adequacy assessment.[134] As already mentioned, China is an important commercial partner for EU, but there has also been substantial political tension between the parties throughout the years. The system of government in China differs to the ones prominent within the EU member states, and China holds different views on important values such as democracy and the principle of popular sovereignty.

Yet, an annual EU-China summit is being held every year to discuss the political and economic relationship between the parties. Despite the differences mentioned above, this demonstrates how both China and EU are putting in an effort to sustain and improve the relationship.

[133] CSL Article 12 (2)
[134] EC MEMO/17/15

6. Summary

Finally, this section will briefly summarize the above assessment and elucidate the chances that the Chinese data protection framework can be deemed "essentially equivalent"[135] in accordance with the GDPR Article 45 and *Schrems v. Data Protection Commissioner*? In other words; how realistic the possibilities of an adequacy decision adopted on China are.

The legal framework concerning data protection in China is in fast development and is making progress towards an adequate level of protection in accordance with the GDPR Article 45. As showcased in section 4, Chinese data protection framework has many similarities with the GDPR, even offering more stringent rules regarding important elements such as processing of sensitive data. The adoption of the adequacy decision on Japan demonstrated how minor differences in the legal framework in the third country will not necessarily dismiss the chance of the adoption of an adequacy decision. In the event of future talks regarding an adequacy decision, it would be a possibility for China to make amendments to their existing framework to assure compliance with the GDPR, as Japan did by implementing new legislation simultaneously as the implementation of the adequacy decision.

As the portrayal has shown, the Chinese framework has been complex making it difficult to navigate both relevant provisions and the responsible authorities. Evidently, this has improved during the past couple of years with the introduction of CSL and the Standard, in addition to improving the coordination of supervision authorities subordinated CAC.

However, the lack of safeguards preventing public authorities from having the opportunity to gain access to personal data on a general basis constitutes an obstacle in relation to the possibility of an adequacy decision on China. Making sure such safeguards exist and are effectively enforced is not only a criterion in accordance with GDPR Article 45 (2) (a), but was proved to be a crucial element in order for an adequacy decision to be valid in accordance with *Schrems v. Data Protection Commissioner*.

[135] *Schrems v. Data Protection Commissioner*, C-362/14, paras. 73-74

Reference list

Literature

Greenleaf (2018)	Greenleaf, Graham, "Japan and Korea: Different paths to EU adequacy", 156 Privacy Laws & Business International Report, December 2018, p. 9-11 Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3323980> Last accessed 9 December 2018
Han and Munir (2018)	Han, Sarah Wang and Munir, Abu Bakar, "Information Security Technology – Personal Information Security Specification: China's Version of the GDPR", European Data Protection Law Review (EDPL) 4, no. 4, 2018, p. 535-541
Lenaerts and van Nuffel (2011)	Lenaerts, Koen and van Nuffel, Piet, "European Union Law", 3rd edition, Sweet & Maxwell, 2011
Udsen (2019)	Udsen, Henrik, *IT-RET* [*IT-LAW,* my translation], 4th edition, Ex Tuto Publishing, 2019

EU Legislation

Directive 95/46	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('Directive 95/46')
Directive (EU) 2016/680	Directive (EU) 2016/680 of the European Parliament and of the Council f 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/89
TFEU	The Treaty on European Union and the Treaty on the Functioning of the European Union
The Charter	Charter of Fundamental Rights of the European Union 2012/C 326/02
The GDPR	Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of

	such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) [2016] OJ 2 119/1
2000/517/EC	Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C(2000) 2304), 2000/517/EC, OJ L 215/01
2002/2/EC	Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539), 2002/2/EU, OJ L 002/13
2003/490/EC	Commission Decision of 30 June 2003 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy protection of personal data in Argentina, 2003/490/EC, OJ L 168/19
2003/821/EC	Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey (notified under document number C(2003) 4309), 2003/821/EC, OJ L 308/27
2004/411/EC	Commissions Decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man (notified under document number C(2004) 1556), 2004/411/EC, OJ L 151/48
2008/393/EC	Commission Decision of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey (notified under document number C(2008) 1746), 2008/393/EC, OJ L 138/21
2010/146/EU	Commission Decision of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data (notifies under document C(2010) 1130), 2010/146/EU, OJ L 58/17
2010/625/EU	Commission Decision of 19 October 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra (notified under document C(2010) 7084), 2010/625/EU, OJ L 277/27
2011/61/EU	Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with

	regard to automated processing of personal data (notified under document C(2011) 332), 2011/61/EU, OJ L 27/39
2012/484/EU	Commission Implementing Decision of 21 August 2012 persuant to Directive 95/46/EU of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic Uruguay with regard to automated processing of personal data (notified under document C(2012 5704), 2012/484/EU, OJ L 277/11
2013/65/EU	Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand (notified under document C(2012) 9557), 2013/65/EU, OJ L 28/12
(EU) 2016/1250	Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S Privacy Shield (notified under document C(2016) 4176, OJ L 207/1
(EU) 2019/419	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 adequacy protection of personal data by Japan under the Act on Protection of Personal Information (notified under document C(2019) 304), OJ L 76/1

Chinese legislation

CSL	Cybersecurity Law of The People's Republic of China **English translation:** Creemers, Trilio and Webster, "Translation: Cybersecurity Law of the People's Republic of China [Effective June 1, 2017]", New America, 29 June 2018 <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/> Last accessed 20 November 2019
GB/T 22239 - 2019	Information Security Technology – Baseline for classified protection of cybersecurity <http://www.gbstandards.org/GB_standard_english.asp?code=GB/T%2022239-2019&word=Information%20security%20technolog> Last accessed 8 December 2019

GB/T 25070 – 2019	Information Security Technology – Technical requirements of security design for classified protection of cybersecurity <http://www.gbstandards.org/GB_standard_english.asp?code=GB/T%2025070-2019&word=Information%20security%20technolog> Last accessed 8 December 2019
GB/T 28448 – 2019	Information Security Technology – Evaluation requirements for classified protection of cybersecurity <http://www.gbstandards.org/GB_standard_english.asp?code=GB/T%2028448-2019&word=Information%20security%20technolog> Last accessed 8 December 2019
National Intelligence Law	National Intelligence Law of The People's Republic of China **English translation:** "National Intelligence Law of P.R.C. (2017)", China Law Translate, 27 June 2017 <https://www.chinalawtranslate.com/%e4%b8%ad%e5%8d%8e%e4%ba%ba%e6%b0%91%e5%85%b1%e5%92%8c%e5%9b%bd%e5%9b%bd%e5%ae%b6%e6%83%85%e6%8a%a5%e6%b3%95/?lang=en> Last accessed 7 December 2019
PCPPIC	Provisions on Cyber Protection of Children's Personal Information **English summary:** "China Issues Provisions on Cyber Protection of Children's Personal Information", Hunton Andrews Kurth, 7 October 2019 <https://www.huntonprivacyblog.com/2019/10/07/china-issues-provisions-on-cyber-protection-of-childrens-personal-information/> Last accessed 20 November 2019 **Official Chinese Version**: http://www.cac.gov.cn/2019-08/23/c_1124913903.htm
The Measures	Personal Information Outbound Transfer Security Assessment Measures **English translation:** "Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China, 'Personal Information Outbound Transfer Security Assessment Measures (Draft for Comment)'", New America, 13 June 2019 <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/> Last accessed 21 November 2019 **Official Chinese Version:** <http://www.cac.gov.cn/2019-06/13/c_1124613618.htm> Last accessed 21 November 2019

The Standard	Information Technology – Personal Information Security Specification, BG/T 35273-2017 **English translation:** "Translation: China's Personal Information Security Specification", New America, 8 February 2019 <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/> Last accessed 25 November 2019

Case law

Azevedo and Others	Judgement 15 December 2016, *Azevedo and Others*, C-558/15, EU:C:2016:957
Lindqvist	Judgement 6 November 2003, *Lindqvist*, C-101/01, EU:C:2003:596
Schrems v. Data Protection Commissioner	Judgement 6 October 2015, *Schrems v. Data Protection Commissioner,* C-362/14, EU:C:2015:650
van Adverteerders	Judgement 26 April 1988, *van Adverteerders,* C-352/85, EU:C:1988:196

Soft law

COM/2012/011 final	Proposal 25 January 2012 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM/2012/011 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012PC0011> Last accessed 30 November 2019
EC MEMO/17/15	Commission, "Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers", Press Release MEMO/17/15, 10 January 2017 <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_15> last accessed 20 November 2019
EC Press Release (2019)	Commission, "European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows", Press release, 23 January 2019 <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421> last accessed 20 November 2019

EC Press Release (2018)	Commission, "The European Union and Japan agreed to creat the world's largest area of safe data flows", Press release, 17 July 2018 <https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4501> last accessed 20 November 2019
EC Statement (2017)	Commission, "Joint Declaration by Mr. Shinzo Abe, Prime Minister of Japan, and Mr. Jean-Claude Juncker, President of the European Commission", Statement, 6 July 2017 <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_17_1917> last accessed 20 November 2019
EDPB Guidelines 3/2018	The European Data Protection Board, "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation, Adopted on 16 November 2018" <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf> last accessed 19 November 2019
EDPB 5th Plenary session	European Data Protection Board, "Fifth Plenary Session: EU-Japan draft adequacy decision, DPIA lists (DK, HR, LU, and SI), and guidelines on accreditation", 5 December 2018 <https://edpb.europa.eu/news/news/2018/european-data-protection-board-fifth-plenary-session-eu-japan-draft-adequacy-decision_en> last accessed 20 November 2019
EP Resolution (2018)	Parliament, "Motion for a resolution to win up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection of personal data afforded by Japan", 10 December 2018, B8-0561/201 <https://www.europarl.europa.eu/doceo/document/B-8-2018-0561_EN.pdf?redirect> last accessed 20 November 2019
JCD No 154/2018	Decision of the EEA Joint Committee No 154/2018 6 July 2018, L 183/23
WP 254 rev.01	Article 29 Working Party, "Adequacy Referential", Revised 6 February 2018, WP 254 rev.01 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108> last accessed 20 November 2019
WP 243 rev.01	Article 29 Working Party, "Guidelines on Data Protection Officers ('DPOs')", Revised 5 April 2017, WP 243 rev.01 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048> Last accessed 20 November 2019

Websites

China Law Blog — China Law Blog, "China´s New Cybersecurity Program: NO Place left to hide" <https://www.chinalawblog.com/2019/09/chinas-new-cybersecurity-program-no-place-to-hide.html> Last accessed 9 December 2019

CMS — CMS, "China publishes the National Cybersecurity Incident Response Plan", 28 June 2017 <https://www.cms-lawnow.com/ealerts/2017/06/china-publishes-the-national-cybersecurity-incident-response-plan?cc_lang=de> Last accessed 9 December 2019

EC, "Adequacy decisions" — The European Commission, "Adequacy decisions, How the EU determines if a non-EU country has an adequate level of data protection" <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> last accessed 20 November 2019

EC, "China" — The European Commission, "China" <https://ec.europa.eu/trade/policy/countries-and-regions/countries/china/> last accessed 20 November 2019

EC, "Communications" — The European Commission, "Communication" <https://ec.europa.eu/info/departments/communication_en> last accessed 24 November 2019

EC, "EU-wide coordinated risk assessment of 5G networks security" — The European Commission, "EU-wide coordinated risk assessment of 5G networks security" <https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security> Last accessed 9 December 2019

EC, "Overview of FTA and Other Trade Negotiations" — The European Commission, "Overview of FTA and other Trade Negotiations" <https://trade.ec.europa.eu/doclib/docs/2006/december/tradoc_118238.pdf> Last accessed 9 December 2019

EDPB, "Role of the EDPB" — European Data Protection Board, "Role of the EDPB" <https://edpb.europa.eu/role-edpb_en> Last accessed 9 December 2019

ICO, Denham (2019) — Denham, Elisabeth "Blog: How will personal data continue to flow after Brexit?", Information Commissioner's Office, 10 September 2019 <https://ico.org.uk/about-the-ico/news-and-events/blog-how-will-personal-data-continue-to-flow-after-brexit/> last accessed 19 November 2019

NOYB (2018) NOYB, "GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook", 25 May 2019 <https://noyb.eu/4complaints/> Last accessed 9 December 2019

Triolo and others (2017) Triolo, Paul and others, "China's Cybersecurity Law One Year On", New America, 30 November 2017 [Blog post] < https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/>

Zhang and Yin (2019) Zhang, Gil and Yin, Kate, "More updates on the Chinese data protection regime in 2019", International Association of Privacy Professionals (IAPP), 25 February 2019 <https://iapp.org/news/a/more-positive-progress-on-chinese-data-protection-regime-in-2019/> Last accessed 21 November 2019

News articles

BBC News, "GDPR: US news unavailable to EU users under new rules", BBC News, 25 May 2018, <www.bbc.com/news/world-europe-44248448> last accessed 19 November 2019

China Daily "Student suffers fatal cardiac arrest after telephone scam", China Daily, 25 August 2016 <https://www.chinadaily.com.cn/china/2016-08/25/content_26591216.htm> last accessed 20 November 2019

China.org.cn "Telecom fraud claims life of another student", China.org.cn, 26 August 2016 <http://www.china.org.cn/china/2016-08/26/content_39173779.htm> last accessed 22 November 2019

Chin, Josh Chin, Josh, "Chinese regulator rebukes Ant Financial for automatic credit scoring enrollment", Privacy International, <https://privacyinternational.org/examples/1956/chinese-regulator-rebukes-ant-financial-automatic-credit-scoring-enrollment> Last accessed 22 November 2019