Higher Education (2019) 78:911–930
https://doi.org/10.1007/s10734-019-00377-5

The New Silk Road: a bumpy ride for Sino-European collaborative research under the GDPR?

Stijn van Deursen[1,2] · Henk Kummeling[1]

Published online: 27 March 2019

Abstract
The Chinese New Silk Road initiative offers unique opportunities for setting up Sino-European research collaborations. Academic cooperation between countries that are rooted in completely different legal, cultural, and academic backgrounds might however also create new challenges. This article investigates the impact of these differences in the field of the protection of personal data, which is a topic that is currently high on the EU's agenda. Whereas the protection of personal data is engrained in the European Union's legal framework, this is not the case in China. This might be problematic, given the fact that scientific collaboration often entails the exchange of (sensitive) personal data. We explore to what extent the General Data Protection Regulation still allows the transfer of such data for scientific purposes to China. After having analyzed the Chinese system in light of the European legislation, we conclude that the sharing of personal data with China is challenging at a minimum. Until more stable legal arrangements are set up in order to facilitate such practices, it is important to share only anonymized data or to acquire consent of the data subject.

Keywords Research collaboration · Personal data · GDPR · China · European Union

A New Silk Road through the dynamic field of international research collaboration

The world of international collaborative research is rapidly changing: recent events such as Brexit and the US turning its back to international cooperation have led to a tendency to restrict free

Stijn van Deursen is researcher at the Utrecht University School of Law and student of the Legal Research Masters. Henk Kummeling is Distinguished University Professor Constitutional Law and Rector of Utrecht University. Both authors are researchers involved in the international New Silk Road research project. See for more information: www.academicsilkroad.org and www.uu.en/en/organisation/centre-for-global-challenges/projects/the-new-silk-road. Research for this contribution ended on 25 February 2019.

✉ Stijn van Deursen
s.vandeursen@uu.nl

[1] Utrecht University, Utrecht, The Netherlands

[2] Utrecht University, Heidelberglaan 8, 3584 CS Utrecht, The Netherlands

flows of knowledge, ideas, and students (Hille 2018; Kirby and Van der Wende 2019). At the same time, China has launched its New Silk Road initiative (also known as the One Belt One Road project, or Belt and Road Initiative). The New Silk Road initiative is aimed at a further integration of China and countries in, among others, Europe, Asia, and Africa. Although the initiative is to a large extent aimed at establishing traditional infrastructure, such as bridges and railways, it also seeks to strengthen digital connections (see, for example, Economist 2018; Deeks 2018). These developments have the potential to integrate major parts of the world, but it is not entirely clear under what conditions this will take place and who will define these conditions (see also Kirby and Van der Wende 2019).

There are several reasons to assume that the New Silk Road will influence both higher education and research in Europe and beyond, as also identified by, among others, Kirby and Van der Wende (2019, p. 129) First of all, just like the ancient silk road, the New Silk Road and its digital infrastructures will not only carry goods and persons but also knowledge and ideas. Secondly, Kirby and Van der Wende describe the rise of China as a global power as one of the most important geopolitical trends of the early twenty-first century. Just like previous major geopolitical events—such as the Second World War, the creation of the EU, and the fall of the Berlin wall—had a considerable impact on higher education and research, it seems likely that the New Silk Road will impact the world of higher education and research. Finally, the Chinese system of research and development is rapidly advancing (see for recent developments of the GDP spending on R&D in China in comparison to the EU and the USA: OECD 2019a, and for such data for R&D intensity: OECD 2019b; Economist 2019b; Van der Wende and Tijssen 2019). Such developments might influence both China's regional partners, but also its global competitors (Kirby and Van der Wende 2019, p. 129). Moreover, alongside the New Silk Road, several projects are set up which are specifically aimed at fostering academic collaboration, such as the University Alliance of the Silk Road and the Belt and Road Platform to Promote Innovation. At the same time, collaborative research with China is one of the priorities in the international research agenda at both European Union level as well as in the European Member States (see, for example, the agreement for scientific and technological cooperation between the European Community and the Government of the People's Republic of China; The EU-China 2020 Strategic Agenda for Cooperation; EU Delegation to China and Mongolia 2014; D'Hooge et al. 2018, pp. 13–14). Although Chinese universities are thus flourishing in many ways and cooperation can therefore create unique academic opportunities, there are also challenges connected to collaborative research between institutions in countries that are rooted in different cultural, legal, and academic backgrounds (Kirby and Van der Wende 2018, p. 128). The New Silk Road might therefore also provide a bumpy ride. The international New Silk Road research project, in which both authors are involved as researchers, investigates China's rise in global higher education and its possible implications for higher education and research cooperation between China and Europe.[1] It does so in four main areas of inquiry: the trends in academic traffic on the New Silk Road; the response of the higher education institutions to new opportunities; the conditions under which these activities can take place and finally the values that underpin the idea of the university and its role in international collaboration.

In this contribution, we enter the third area of inquiry by focusing on the question of to what extent the current European conditions on protecting and sharing personal data allow for transferring such data to China in the context of collaborative research. This is an important question because, as also mentioned by European Data Protection Supervisor Giovanni

[1] www.academicsilkroad.org and www.uu.en/en/organisation/centre-for-global-challenges/projects/the-new-silk-road. The project will be concluded with an international conference in Germany in May 2020.

Buttarelli in his 2016 speech, data can be seen as the fuel and catalyst of innovative research: sharing data with research partners is a pledge of trust and a sign of mutual confidence and respect, and can lead to new and innovative results (Buttarelli 2016). Thereby, data have the potential to save lives (DG Internal Policies 2016). At the same time, unregulated use of data relating to individuals can have considerable negative impacts for these individuals, such as identity theft or discrimination. In the European Union, these risks are mitigated by the fundamental right to the protection of personal data, which forms part of the European constitutional fabric. The right to the protection of personal data is operationalized in the General Data Protection Regulation (GDPR). In China, however, such a right does not seem to be explicitly incorporated in the legal system. Such differences should, however, in our view not lead to a direct rejection of all cooperation with China. The answer to the question of how much cooperation is possible should rather be based on a clear strategy and an assessment of the risks, challenges, and benefits that are involved (see also D'Hooge et al. 2018, iv; Economist 2019a). In this contribution, we explore this balance between scientific development and the protection of individual's personal data.

In order to answer the question of to what extent the current European framework allows for a transfer of personal data to China for scientific purposes, this contribution firstly provides a short introduction into the GDPR, its place in the legal landscape of the European Union, and its regime with regard to personal data gathered in research situations ("The GDPR's consequences for collaborative research"). Then the focus shifts to a description of the GDPR's approach with regard to the transfer of personal data to third countries ("The GDPR's regime for third country transfers of personal data for scientific purposes"). In the following section, a brief comparative glance at the Chinese data protection regime is provided. The "Future directions for transporting personal data over the New Silk Road" section subsequently addresses the potential obstacles arising out of the different approaches of both the EU and China with regard to the protection of personal data in the context of scientific research and provides further directions for sharing such data with China. Because of our focus on activities falling within the scope of the GDPR, we do not focus on the flow of personal data from Chinese entities or data regarding Chinese citizens to the EU, although this might also pose interesting and fundamental legal and ethical challenges.

The GDPR's consequences for collaborative research

Many types of scientific research concern information that can either directly or indirectly be related to individuals. This might be both information on research subjects and information on researchers themselves. In the Member States of the European Union, the protection of such personal data is considered a fundamental right, which was first implicitly laid down in Art. 8 of the European Convention of Human Rights (ECHR) and later more explicitly in Convention 108 of the Council of Europe and in Art. 8 of the Charter of Fundamental Rights of the European Union.[2] Since 1995, this right was inter alia operationalized in Directive 95/46/EG on the protection of individuals with regard to the processing of personal data and on the free

[2] Art. 8 ECHR provides that "[e]veryone has the right to respect for his private and family life, his home and his correspondence." See for an overview of the role of this article in protection personal data also ECtHR 2018. Art. 8 CFR explicitly lays down that "[e]veryone has the right to the protection of personal data concerning him or her." Convention 108 of the Council of Europe provides rules for the protection of individuals with regard to the automatic processing of personal data.

movement of such data (hereinafter, Data Protection Directive). This directive aimed to ensure that personal data could flow freely from one European Member State to another, while at the same time safeguarding the fundamental rights and freedoms of individuals (Art. 1 and Recitals 1–9, Data Protection Directive; Voigt and Von dem Bussche 2017, p. 2). To do so, the Data Protection Directive not only provided rules on the processing of personal data within the European Union but also for the transfer of such data to countries and international organizations outside the European Union (Chapter IV, Data Protection Directive). However, a general characteristic of European directives is that they are only binding with regard to their objective and that they are not directly applicable in the European Member States (Art. 288(3) Treaty on the Functioning of the European Union). In order to reach their objective, directives therefore have to be implemented in the national legal orders of the European Member States. The Member States are generally free to choose the specific means that they use in order to do so (Barnard and Peers 2014, p. 99). For the Data Protection Directive, this entailed that—although the (main) objective of ensuring a balance between the free flow of personal data and the protection of fundamental rights was binding—it was left to the authorities of the EU Member States to choose the actual form and methods that were used in order to achieve this objective.[3] The discretionary space that was left to Member States resulted in a patchwork of national approaches (Recital 9 GDPR; Voigt and Von dem Bussche 2017, p. 2; Handbook on EU Data Protection Law 2018, p. 30).

In 2010, the European Commission reviewed this European framework of data protection and concluded that the Data Protection Directive could not live up to all of its objectives. The plethora of approaches in the European Member States led to differences in "assessing the level of adequacy of [safeguarding data protection rights in] third countries, or international organisations, and involves the risk that the level of protection of data subjects provided for in a third country is judged differently from one Member State to another" (European Commission 2010, p. 15). This unclarity with regard to the transfer of personal data to countries outside of the European Union was one of the reasons that necessitated a new legal instrument according to the Commission (European Commission 2010, p. 15).[4]

Because the objectives of the Directive were at the same time still considered to be valid, the Commission stated that the identified challenges required "the EU to develop a comprehensive and coherent approach guaranteeing that the fundamental right to data protection for individuals is fully respected within the EU and beyond" (European Commission 2010, p. 4). This desired comprehensive and coherent approach was made possible by the adoption of new primary legislation, which came into force after the adoption of the Data Protection Directive in 1995 and provided the European legislator with a stronger legal basis in primary Union law.[5]

[3] Art. 288(3) TFEU. The Data Protection Directive allowed for a certain margin for maneuver, which was also at issue in Case C-101/01 *Lindqvist* ECLI:EU:C:2003:596 [2003] (especially in para 97). In order to safeguard coherence under the Data Protection Directive, the so-called Article 29 Working Party was set up as an advisory body.

[4] For more on the evaluation of the framework on data protection under the Data Protection Directive, see Robinson et al. (2009) and Recital 9 GDPR.

[5] The most important of which are Art. 16(2) TFEU and Art. 8 Charter of fundamental Rights of the European Union. Art. 16(2) TFEU provides that "The European Parliament and the Council, (…), shall lay down the rules relating to the protection of individuals with regard to the processing of personal data (…), and the rules relating to the free movement of such data." Art. 8 CFR explicitly incorporates a fundamental right to the protection of personal data into the legal order of the European Union.

After a lengthy legislative procedure, Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) was adopted in 2016. First of all, contrary to the Data Protection Directive, the GDPR is not a directive but a regulation which therefore has general application; it is binding in its entirety and since 25 May 2018 directly applicable in all EU Member States. On specific points, the GDPR requires further national rules in order to ensure its full effectiveness. See, for example, of the use of this discretionary space by Member States in the field of research also paragraph 3.1 of this contribution. By this approach, the GDPR seeks to ensure a "consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union" (Recital 10 GDPR). In order to do so, compared to the Data Protection Directive, the GDPR is not only more focused at ensuring compliance by requiring new compliance mechanisms but also introduces stronger rights and enforcement measures for data subjects.[6]

The GDPR is applicable to the processing of any data relating to natural persons if this takes place by an entity that is established in the EU or in case these data relate to EU individuals.[7] Crucial terms with regard to the applicability of the GDPR are therefore that of *personal data* and the *processing* thereof.

Personal data are any information that is or can be related to an identified or identifiable living person: the data subject (Art. 4(1) GDPR). An identifiable natural person is subsequently defined by the GDPR as "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[8] In case law of the Court of Justice of the European Union, the concept of *information* has been interpreted broadly: it also includes subjective matters such as opinions or assessments, which can be seen as reflections of an individual's intellect, thought processes, and judgments.[9] Moreover, the notion of personal data also includes information which can be *indirectly* related to a natural person, for example, by using additional information, data sets, or "all the means reasonably likely to be used."[10] In order to determine whether certain means are reasonably likely to be used, all objective factors should be taken into account. This includes factors such as costs, time, and

[6] The GDPR, for example, introduces a stronger regime for compliance and accountability (Art. 24 GDPR), the protection of privacy by design (Art. 25 GDPR), and new risk assessment methods (Art. 35 GDPR), and requires certain entities to designate a Data Protection Officer (Art. 37 GDPR). New data subject rights include a right to data portability (Art. 20 GDPR), a right to be forgotten (Art. 17 GDPR; however, in case law of the CJEU, such a right was already recognized: Case C-131/12 *Google Spain* [2014]), and a right to damages in case of a breach of data protection obligations (Art. 82 GDPR).

[7] Art. 2–4 GDPR.

[8] Art. 4(1) GDPR.

[9] Case C-434/16 *Peter Nowak* ECLI:EU:C:2017:994 (2017) para 34 and 37. See also Art. 29 Working Party, "The concept of personal data" (Opinion 4/2007), 6. Under the GDPR, the Article 29 Working Party is succeeded by the European Data Protection Board (EDPB). Just like the Article 29 Working Party, the main task of the EDPB is to watch over the consistent application of the GDPR. In a number of endorsements, the EDPB has confirmed the work of the Article 29 Working Party that relates to the GDPR. The EDPB has not expressed itself on other work of the Article 29 Working Party, such as on this opinion. However, under the GDPR, the definition of personal data has not changed compared to the Data Protection Directive. Therefore, in our view, the Article 29 Working Party's opinion the concept of personal data is still valid.

[10] Recital 26 GDPR. See, for an example, of identifying natural persons by using statistical data: Narayanan and Shmatikov 2008 (using statistical data in order to identify individual Netflix users and uncover, e.g., their apparent political preferences and other potentially sensitive information); Voigt and Von dem Bussche 2017, p. 12.

available technology at the time of processing as well as expected technological developments (Recital 26 GDPR). The concept of personal data is thus broad, which implies for scientific research that in case a study relates to information that can be linked to living individuals, the GDPR is applicable. The applicability of the GDPR to scientific research is also explicitly confirmed by Recital 159, which subsequently introduces the broad interpretation of such research. This covers, for example, not only technological development and demonstration, fundamental research, applied research, and privately funded research but also studies conducted in the public interest in the area of public health, historical research, and research for genealogical purposes. Here, it is important to stress that the GDPR is not applicable to deceased persons (Recitals 159–160).

Probably not surprising, the concept of *processing* is likewise broadly defined by the GDPR and includes not only any operation relating to personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, dissemination or otherwise making available, but also erasure or destruction (Art. 4(2) GDPR). Seen in light of the aforementioned broad definition of personal data, this implies that virtually any use of information on the basis of which a living natural person can be identified is covered by the GDPR. This therefore also includes almost all use of information relating to individuals in scientific contexts. It is, however, important to bear in mind that data that are anonymized—i.e., data that cannot be traced back to a natural person—do not fall within the scope of the GDPR. The relevance thereof is further discussed in the section focusing on the "Processing of personal data for research purposes under the GDPR".

In case of collaborative research involving multiple research institutions, the GDPR is firstly applicable if one of the research institutions involved in the transfer of personal data is established in the European Union.[11] Secondly, the GDPR applies as well in case the research institution is established outside of the European Union while the processed data relate to data subjects that are in the European Union, or if the data relate to the behavior of data subjects within the European Union (Art. 3 GDPR).

The GDPR's regime for third country transfers of personal data for scientific purposes

The transfer of personal data to China, a country that is not part of the European Union, has to comply with the regime laid down in Art. 44 GDPR and further. This basically requires that the level of protection that is offered to personal data in the European Union may not be undermined by the transfer of such data.

The assessment of a transfer of personal data to either an international organization or to a third country exists of two stages. First of all, a transfer is a form of processing and therefore has to comply with the requirements for processing of the GDPR. This step therefore concerns the *transferring process*. Secondly, the transfer should be surrounded with sufficient

[11] This presupposes that the university is able to determine the purposes and means of the processing of personal data and therefore qualifies either as controller or as joint-controller (Art. 4(7) and Art. 26 GDPR). In most situations, this will indeed be the case. According to the Article 29 Working Party, in order to provide data subjects with a more stable and reliable entity for the enforcement of their rights, preference should be given to consider a company as controller, rather than a specific person within that company (Article 29 Data Protection Working Party 2010, p. 15). In most cases, the institution for which an individual researcher is working will therefore qualify as controller.

safeguards in order to make sure that the international organization or third country in question provides an adequate level of protection. Hence, this step focuses on the situation in the *recipient third country*.

Processing of personal data for research purposes under the GDPR

Under the GDPR's broad definition of processing, the transfer of personal data for scientific purposes is regarded as a form of processing that should therefore comply with the substantive norms of the GDPR.[12] This means that all processing of any type of personal data should be done in accordance with the data processing principles of the GDPR. The GDPR applies a stricter regime for the processing of special categories of personal data, which is information revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, (…) genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" (Art. 9(1) GDPR). The processing of such data, which is not unlikely in the context of scientific research collaboration, is in principle prohibited. Think, for example, of such practices of research concerning biomedical or genetic data, but also of sociological research relating to political opinions, trade union memberships, or religious affiliations which can, either directly or indirectly, be traced back to specific individuals. Exceptions to the prohibition of the processing of specific categories of personal data are listed in Art. 9(2) GDPR. One of these exceptions has to apply in addition to the data processing principles for the processing of this type of data to be legitimate.

The processing of all personal data, so therefore including special categories of personal data, should be done in accordance with all the data processing principles of Art. 5 GDPR. In the following, we briefly address these principles and their relevance for the processing of personal data for research purposes. In case the processing of personal data cannot be done in accordance with the GDPR data processing principles, processing of such data is not allowed and the information will have to be anonymized. See for a detailed analysis of the requirements for anonymization the Article 29 Working Party opinion on anonymization techniques (2014).[13]

First of all, the processing of personal data should be done in accordance with the principles of lawfulness, fairness, and transparency (Art. 5(1)(a) GDPR; Handbook on European data protection law 2018, pp. 117–122). Under the principle of lawfulness, processing of personal data for research purposes can be based on consent of the data subject. Consent should be given freely, which means that it should be based on genuine or free choice and that one should be able to refuse or withdraw consent without detriment (Recital 42 GDPR). It is therefore important to make sure that there are no other reasons for the data subject to consent, such as potential access to experimental medicine related to participation in a research.[14] Furthermore,

[12] A useful schematic overview of these requirements for research purposes can be found via https://www.eur.en/sites/corporate/files/2017-11/How_to_treat_personal_data_in_research_1.0.pdf (accessed 25 February 2019).
[13] On the validity of the opinions of the Article 29 Working Party under the GDPR, see also footnote 10.
[14] In case of clinical trials, consent should according to Recital 161 GDPR also comply with the regulation on clinical trials on medicinal products for human use (Regulation (EU) No 536/2014), defining informed consent as "a subject's free and voluntary expression of his or her willingness to participate in a particular clinical trial, after having been informed of all aspects of the clinical trial that are relevant to the subject's decision to participate or, in case of minors and of incapacitated subjects, an authorisation or agreement from their legally designated representative to include them in the clinical trial."

consent should be informed, unambiguous, and specific. However, when data are processed for research purposes, it is often hard to define the exact research purposes on beforehand. The GDPR therefore also allows for consent to a research in accordance with recognized ethical standards for scientific research (Recital 33 GDPR. Consider, e.g., The European Code of Conduct for Research Integrity). For the transfer of personal data to a third country, this therefore entails that the relevant ethical standards should also be upheld in the country in question. Finally, there are some practical issues connected to the processing of personal data for research purposes on the basis of consent under the GDPR. Science Europe has, for example, made clear that for some research purposes, it may be hard or even impossible to acquire consent, such as in observational research studies where the sample size can be very large (Science Europe 2016). Moreover, a data subject has the right to withdraw his or her consent on the basis of Art. 7(3) GDPR, which can make this a rather unstable ground for processing. Higher thresholds apply for the processing of special categories of personal data. For the processing of special categories of personal data, Art. 9(2) (a) GDPR provides that normal consent does not suffice, but that on top of the aforementioned requirements, explicit consent is required.

The processing of personal data for research purposes is also possible on the basis of Art. 6(1)(f) GDPR. Under this article, personal data may be processed in case this is necessary for the purposes of the legitimate interests pursued by the research institution or by a third party. These interests should however be balanced against the interests or fundamental rights and freedoms of the data subject. Art. 6(1)(f) GDPR offers additional protection to children; the processing of their personal data therefore seems to be less viable on the basis of this balancing act. A similar balance of interests with regard to the processing of special categories of personal data for research purposes can be found in Art. 9(2)(j) GDPR, although the stakes in this balancing act are higher. Under this article, processing is allowed in case there is a basis for doing so in Member State law and if the processing is necessary for research purposes, while the essence of the right to data protection is respected and in case specific measures are taken to safeguard the fundamental rights and interests of the data subject (see also Art. 89(1) GDPR). These measures may include the use of pseudonymization when possible and anonymization of the data as soon as it is not necessary anymore to identify the data subject.[15] The legal basis in Dutch law, for example, provides that processing of special categories of personal data for scientific purposes is possible in case the research serves a public interest and if it is impossible or would require a disproportionate effort to request consent while safeguards are in place to make sure that the data subject's privacy would not be disproportionately jeopardized (Art. 24 Implementing Act GDPR). Germany applies a similar regime, by providing that the processing of special categories of personal data is also possible without consent, if this is necessary for the purposes and interests of the research institution as long as these purposes and interests outweigh the purposes and interests of the data subject (Art. 27

[15] There is a difference between pseudonimyzation and anonymization. Anonymized data cannot be traced back to an individual person and therefore falls outside the scope of the GDPR. Art. 4(5) GDPR defines pseudonymization as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." Pseudonymization, however, is only considered to be a safety measure, existing in, e.g., the coding of names, and therefore the GDPR remains applicable. In this way, pseudonymization is a way to comply with the data protection obligations under the GDPR.

Federal Data Protection Act). Germany thereby does not explicitly require that the research serves a public interest, and thereby seems to be more lenient with regard to personal data processing for research purposes.[16] The different regimes that European Member States may apply with regard to processing of personal data for research purposes may prove to be an obstacle for international research cooperation, as is also pointed out by, among others, the League of European Research Universities (Nicholson 2018).

The principle of fairness requires that the data subject is informed of the risks connected to the processing of his or her personal data, in order to make sure that the processing does not have unforeseeable negative effects. The principle of transparency furthermore requires that data subjects are informed of the processing of their data, the purposes of such processing, and the identity and address of the institution that is responsible for the processing. This information must be provided in a clear way, so that data subjects are able to understand the (legal) context in which their data are being processed. Visualization should be used when appropriate, for example, by using a website informing the data subject on the aforementioned factor. Lastly, data subjects should be able to access their data, although Member State law may under strict conditions provide for derogations to this right in the context of scientific research (Art. 15 and 89(2) GDPR).

Secondly, the principle of purpose limitation requires that the purposes of the processing of personal data are defined in advance and that the processing may not go further than these predefined purposes (Art. 5(1)(b) GDPR). Also on this point, the GDPR provides a specific derogation for the further processing of personal data for research purposes in this article. Under this exception, further processing of such data for research purposes is possible, provided that safeguards for the rights and freedoms of the data subject are applicable to make sure that no more than necessary data are being processed. This may necessitate pseudonymization and anonymization as soon as possible (Handbook on European data protection law 2018, 122–125). This means that in case personal data are collected for goal A, their processing may not go further than is necessary for reaching goal A. During scientific research, however, it may become clear that the data may also be relevant for reaching goal B. If sufficient safeguards are in place, the data may in principle in that case also be processed for goal B.

This brings us to the principle of data minimization, which is the third data processing principle (Art. 5(1) (c) GDPR). Under this principle, the processing of personal data may not go further than what is necessary for the legitimate purpose and may only take place if there are no other means to meet the same objective. This principle thereby may also lead to the conclusion that pseudonymization or other protecting measures are necessary (Handbook on European data protection law 2018, pp. 125–127).

Under the fourth data processing principle, data must be accurate and, where necessary, kept up to date (Art. 5(1) (d) GDPR; Handbook on European data protection law 2018, pp. 127–128). This principle must be implemented in line with the purposes of the processing of the personal data. Sometimes, a research can only build upon data that reflect the state of affairs at a certain moment in time. Updating is then not required. Here again, it depends on the legislation of a specific Member State to what extent a data subject can actually exercise their

[16] For an updated overview of GDPR implementation acts in place in the different Member States, see also https://uk.practicallaw.thomsonreuters.com/w-013-1949?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk (accessed 25 February 2019).

related right to rectification if his or her data are used for scientific research purposes (Art. 89(3) in connection with Art. 16 GDPR).

According to the principle of storage limitation, as laid down in Art. 5(1)(e) GDPR, data must be kept in a form that does not permit the identification of an individual for a longer period than necessary for the purposes of data processing, meaning that the personal data have to be deleted or anonymized as soon as possible. Data that are being processed for research purposes may be stored for a longer period, if appropriate technical and organizational measures have been taken for safeguarding the rights and freedoms of the data subject during this extended storing period. Under Recital 39 GDPR, this requires a periodic review in order to determine whether the data have to be erased (Handbook on European data protection law 2018, pp. 129–130).

Finally, the principles of integrity and confidentiality provide that measures have to be taken in order to prevent unauthorized or unlawful processing and accidental loss, destruction, or damage (Art. 5(1)(f) GDPR; Handbook on European data protection law 2018, pp. 131–134). In order to do so, research institutions should as much as possible make use of privacy by design and by default, meaning that security measures should be integrated in the processing procedure (Art. 25 GDPR). Categories of data of which the breach of security measures might have considerable impact on the rights and freedoms of individuals, such as special categories of personal data, may require more protection (see also Art. 32 GDPR). Relevant factors in this regard are among others whether the processing of the data might give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage (Recital 75 GDPR). Similarly, the processing of special categories of personal data requires more protection, which is also substantiated in the GDPR: processing of such data on a large scale requires a data protection impact assessment to be made (Art. 35(3)(b) GDPR) and in some cases also the designation of a data protection officer on the basis of Art. 37(1)(c) GDPR. The data protection officer has the task to inform and advise the institutions involved in the processing of personal data on their obligations under the GDPR and to coordinate compliance (see further Art. 39 GDPR).

Ensuring a sufficient level of protection

After having determined whether there is a ground for a transfer of personal data to a country outside the EU, the next question is whether the European level of protection of personal data is not undermined by that particular transfer (Art. 44 GDPR; European Commission 2017).

The GDPR contains several possibilities for safeguarding the GDPR's level of protection in case of personal data transfers to third countries. Firstly, a transfer of personal data can take place on the basis of a decision of the European Commission in which it is decided that the third country in question ensures an adequate level of protection (for more on this so-called adequacy decision, see Art. 45 GDPR).[17] When assessing a third country's adequacy of protection, the Commission has to take the complete legal system of the country in question into account, therefore, including elements such as the respect for the rule of law, human rights norms, access to justice, the existence and effectiveness of an independent data protection

[17] See also https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en for a more detailed description of the procedure for granting an adequacy decision and for a list of countries for which the EU has taken an adequacy decision (accessed 25 February 2019).

authority, and the international commitments the third party has entered into (Art. 45(2) GDPR and, related, Recitals 103–107). In its 2015 decision in the case of Maximilian Schrems, the Court of Justice of the European Union further elaborated on the concept of adequacy and establishes additional standards that have to be met in order to grant an adequacy decision.[18] According to this decision, the third country in question does not have to ensure a level of protection that is *identical* to that of the EU. The third country must, however, ensure that its laws and standards offer a level of protection of fundamental rights and freedoms that is *essentially equivalent* to the level of protection offered within the EU under the Data Protection Directive (now the GDPR), seen in light of the European Charter of Fundamental Rights. This level of protection should also be applicable to the public authorities of the third country, and the applicable legislation should offer an individual the opportunity to apply legal remedies for access to and correction of personal data.

Secondly, if no adequacy decision has been taken, a transfer of personal data is possible on the basis of Art. 46 GDPR. Under this article, a transfer is still possible if appropriate safeguards are provided, and on condition that enforceable rights and effective legal remedies for data subjects are available. Such safeguards include legally binding and enforceable instruments between public authorities or bodies, binding corporate rules, or standard contractual clauses between the different parties that are approved by the national supervisory authority (see further Art. 46(2) and (3) GDPR).

In case no adequacy decision has been taken and appropriate safeguards are absent, Art. 49 GDPR provides that a transfer of personal data to a third country is still possible in specific cases, for example, when the data subject has explicitly consented with such a transfer or when the transfer is necessary for protecting the vital interests of the data subject, where the data subject is physically or legally incapable of giving consent.

The European Commission has not taken an adequate decision with regard to China, and on the basis of our information, no procedure for granting such a decision is currently pending before the European Commission.[19] It therefore has to be determined whether a transfer is possible on the basis of either Art. 46 or 49 GDPR. In order to do so, we provide a brief comparative glance at the Chinese data protection regime in the following section. In the section on "Future directions for transporting personal data over the New Silk Road", we analyze the consequences of the Chinese approach for the transfer of personal data from the European Union to China through the lens of the GDPR.

A brief comparative glance at the Chinese regime for data protection

Before providing a comparative glance at the Chinese regime with regard to the protection of personal data, it is important to note that the assessment of the level of protection offered by a data protection regime in a third country cannot be sufficiently conducted within the limits of this contribution (see also, in this regard, Greenleaf 2017b, p. 3). This is especially the case for the Chinese system, which is rooted in a completely different cultural and legal tradition, thereby further complicating any comparison (De Hert and Papakonstantinou 2015, p. 7).

[18] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner and Digital Rights Ireland Ltd* ECLI:EU:C:2015:650 [2015].

[19] For the latest update, see also https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en (accessed 25 February 2019).

Therefore, in this section, we do not aim to provide a complete or exhaustive overview of the Chinese legal system with regard to the protection of personal data. Instead, we paint its main characteristics with a broad brush, by looking through the lens of the GDPR which was introduced in the foregoing sections. Through this approach, we aim to avoid making any normative statements, as we use the GDPR in order to identify possible challenges for transferring personal data to China in collaborative research. As already stated, when analyzing the potential for a transfer of personal data, other circumstances surrounding that transfer should also be taken into account. This section therefore also touches upon broader topics, such as the rule of law and the (legal) position of the individual.

In 2015, a review of the Chinese approach towards the protection of personal data has been conducted by De Hert and Papakonstantinou. They concluded that from the perspective of the European Data Protection Directive (the predecessor of the GDPR), one cannot speak of a proper data protection regime in China. On the one hand, the European regime of data protection has a basis in fundamental rights and is therefore broadly applicable and protects all individuals. On the other hand, the Chinese approach is based on a multitude of provisions which are mostly of instrumental importance for the development of specific sectors—such as e-commerce or public security—or focus on individuals in a specific capacity, such as that of consumer (De Hert and Papakonstantinou 2015, p. 14). In this section, we also take into account the recent developments in the Chinese approach towards the protection of personal data in order to find out to what extent De Hert and Papakonstantinou's conclusions still hold true.

A right to the protection of privacy is contained in Chinese basic law. However, this right is mostly interpreted as a right to dignity, and therefore as not including a right to privacy in the European sense or the GDPR's right to the protection of personal data (Hert and Papakonstantinou 2015, p. 14; Chen et al. 2015, p. 728).[20] Moreover, this right is generally viewed as not justiciable, meaning that it cannot be invoked before a court and therefore leaving the individual potentially empty-handed (De Hert and Papakonstantinou 2015, p. 16; Greenleaf 2014, p. 196). Protection of personal data is however also offered in several provisions in both penal law and civil law, via inter alia Art. 286(1) Criminal Law and several provisions of the 1986 General Principles of the Civil Law and the subsequent 2009 Tort Liability Law. For a more detailed discussion of this legislation, see Ning and Wu (2018, sect. 1.2), Livingston and Greenleaf (2015), and Greenleaf (2017, p. 19; 2017a, p. 9). The aforementioned legislation is still rather ambiguous, as it only provides that personal data have to be protected, but not what this exactly entails and how this should be done. The 2012 Decision on Strengthening Internet Information Protection of the Standing Committee of the National People's Congress further clarifies this for network service providers, by laying down that if network service providers collect or use citizens' individual electronic information, they have to comply with the principles of legality, legitimacy, and necessity and have to indicate the objective, methods, and scope for collection and use of information (De Hert and Papakonstantinou 2015, pp. 19–20). In the following articles of the Standing Committee of the National People's Congress decision, issues such as confidentiality, security, and the rights to request data controllers to delete information, to cease possible infringements or to report to the controlling departments, are introduced. Similar developments can be seen in

[20] For more on the distinction between privacy and data protection from a European perspective, see Kokott and Sobotta (2013).

sector-specific lower level rules, providing data protection requirements for, e.g., banks, medical institutions, and the telecommunication sector (De Hert and Papakonstantinou 2015, pp. 20–21; Ning and Wu 2018, sect. 1.2).

The protection of personal data in the digital sphere is further strengthened by the Cyber Security Law, which entered into force on 1 June 2017. This law of the Standing Committee of the National People's Congress adds clearer definitions of the fundamental concepts in data protection law and also introduces processing principles similar to those found in the EU, such as that of lawful processing, legitimacy, and necessity when collecting and using personal information and the obligation to keep collected information strictly confidential (see also Greenleaf 2017a, p. 2; Maisog and Li 2017; Xia 2017). The Cyber Security Law is further clarified in the Personal Information Security Specification, which entered into force on 1 May 2018 (Sacks 2018b). Although the Cybersecurity Law and the Personal Information Security Specification certainly raise the level of protection of personal data (Sacks 2018a; Sacks 2018b), the exact interpretation of their concepts is still debated (Sacks et al. 2017; Sacks 2018b, sect. 2). Moreover, the scheme still does not provide for a right of access for data subjects, data quality requirements, or a specific regime for sensitive data. Furthermore, its exact scope of application—especially in the public sector—remains unclear (Greenleaf 2017a, pp. 2–3).

The Chinese government has also acknowledged the importance and potential of research on the basis of genetic material and biobanks, and has enforced legislation in order to protect related personal data. Although this legislation is criticized for its possible narrow scope and for the fact that it is argued to be mainly focused on stimulating scientific competitiveness, it also seems to have importance for the protection of personal data, especially seen in connection with the Guidelines of the Shanghai Biobank Network (Chen et al. 2015).

It is against the background of the aforementioned developments, however, that two experts on Chinese Law—Chao Jing and Tom Zwart—provide a different perspective on the Chinese situation.[21] They reported to us that, in their view, the current legal state of affairs in China regarding data protection already meets the GDPR requirements to a large extent, since data protection is being guaranteed by a number of specific laws. In addition, they argue that—although it is true that the right to privacy as laid down in Article 40 of the Constitution is non-justiciable—the personality rights included in the 2009 Tort Liability Law including the right to data protection, are. Therefore, they do not share what they call "the dim view" expressed by De Hert and Papakonstantinou. Nevertheless, they agree that, with regard to data protection in China, there is "considerable room for improvement". They point at a bill for a Personal Information Protection Law that is currently pending before the Standing Committee of the National People's Congress. According to their information, the bill does not only comprehensively protect the storage and usage of personal data but would also offer individuals the right of access, the right to rectification, and the right to be forgotten to data subjects. The bill would apply to both the public and the private sectors and also introduce a liability scheme. This proposal forms part of the 13th Legislative Plan of the Standing Committee of the National People's Congress and on 7 September 2018; the Standing Committee has awarded "Class 1" status to it, which means that it will be enacted during the current five-year

[21] We asked for their expert opinion on one of the initial drafts of this contribution. They sent their report to us on 25 September 2018. Chao Jing is a PhD student at Utrecht University and specializes in the influence of national security on human rights in among others China. Tom Zwart is a professor in cross-cultural law at Utrecht University.

legislative plan, running until 2023.[22] This, of course, could all be positive news, but it remains to be seen whether the new bill would really offer the required extra legal protection, let alone if it would offer this protection in time.

At this point, it is important to further discuss the setting in which any type of legislation in China has to be put into effect. Although the development of legislation in the field of data protection looks promising, there are also some more critical remarks to be made. First of all, there is no single independent authority in place to supervise compliance with the data protection rules. There are many sector-specific authorities related to, for example, government departments, but it is argued that the scope of their jurisdiction is not clear (Ning and Wu 2018, sect. 1.4; Sacks 2018b; Dong 2018, sect. VII). This results in conflicts about which institution has control and who has the power to give a final interpretation (Sacks et al. 2017; Sacks 2018b, sect. 2 and conclusion). In line with this, from a GDPR perspective, some critical remarks can be made with regard to these authorities' independence, given their often strong ties with other government institutions. As an independent supervisory authority is absent, the protection of individuals is to a large extent dependent upon private enforcement, i.e., on an individual's own decision to bring a case to court. In this regard, it is important to note that Chinese courts are often characterized as "unwelcoming" and to a large extent subject to political instructions (Glenn 2014, p. 351). Moreover, McCuaig-Johnston and Zhang point out that China is a country where "the concept of rights is (…) weakly established and the rule of law is hostage to politics", whereas the protection of both is crucial under the GDPR (McCuaig-Johnston and Zhang 2015, p. 29). A similar development is noticed by Greenleaf, who describes a move away from the rule of law under the Xi Jinping administration towards more political and party control (Greenleaf 2017b, p. 18). Such developments are also noticed in the academic world, where researchers mention increasing political interference in among others the field of research and international cooperation, for example, by increasing difficulties to access the internet, camera's in classrooms, and challenges for scientists and university staff for getting the required visa for working in China (D'Hooge et al. 2018, p. 11). Additionally, the decisions of Chinese judges that have been given are often not binding, not enforced in practice, or contain diverging interpretations (Glenn 2014, p. 352; Dong 2017, sect. VIII). Also, the European Parliament mentions the challenges for a proper data protection system that might result from the lack of democratic conditions for the respect of human rights, such as independent courts, legal certainty, and adequate means of enforcement (European Parliament 2016; see also De Hert and Papakonstantinou 2015, p. 25).

Secondly, the role of the individual in relation to the collective in China differs from the more autonomous role of the individual as it is perceived in European society (Glenn 2014, pp. 336–337). This might have consequences for the application of the exemptions from the protection of personal data in China: the processing of personal data is still allowed for reasons of national security, the public interest, or judicial procedures (Li and Wang 2018). Although such exceptions also exist in European law, the European legislation explicitly requires a balancing act and offers protection to the position of the individual via the role of the judge. Furthermore, given the Chinese legal system's focus on the collective, it seems likely that the collective interest in such a balancing act will often prevail over the individual interest of protection of personal data. Similar concerns are also expressed by European Commissioner

[22] For the latest updates, see https://zh.wikisource.org/wiki/User:NPCObserver/13thNPCSCLegislativePlan (accessed on 25 February 2019).

Violeta Bulc in a 2016 debate in the European Parliament on the transfer of personal data to China (European Parliament debate 7 July 2016).

Finally, we see a worrying development in the increase of governmental control over whole parts of society, especially seen in light of the fact that the current data protection rules are unclear with regard to their applicability to the government (De Hert and Papakonstantinou 2015, p. 15; Greenleaf 2017a, p. 3; Greenleaf 2017b, p. 21). Data—and especially personal data—play an important role in the development of the Social Credit System (Chen and Cheung 2017; Economist 2017), and also on the internet, government is strengthening its grip on personal information (Sacks and Triolo 2017). Similar developments are taking place in the academic sector and thereby create questions on the protection position of personal data, for example, when they are stored in state sanctioned data centers (Normille 2018; Sharma 2018). These concerns are stressed by a 2018 report of the Leiden Asia Centre, quoting a researcher describing that "[i]n China, researchers say they can use the data and promise to protect the data and make sure nothing bad happens with it. But Chinese researchers cannot guarantee that these data might be used by Chinese politicians or civil servants later on" (D'Hooge et al. 2018, p. 22).

Future directions for transporting personal data over the New Silk Road

Besides the fact that the protection of personal data is a fundamental principle in the European Union, which in our view therefore merits strong protection in its own right, the strict sanctioning regime as set out by Art. 83 GDPR might form a stimulus for complying with the GDPR's provisions. Depending on the circumstances of the case, a breach of the GDPR might result in fines up to 20 million euros. Relevant circumstances in this regard are, for example, the nature, gravity, and duration of the infringement, the behavior of the controller, and whether the infringement was intentional. Furthermore, Art. 82 GDPR introduces a right to compensation for both the material and the immaterial damage which is the result of a breach of the GDPR. Therefore, the research institution—that is in most cases in charge of determining the purposes and means of data processing and hence responsible for the processing (see also footnote 11 for more on this topic)—can be held directly liable in case it transfers personal data to a country where these data are insufficiently protected and thereby acts in breach of the GDPR. Compliance with the GDPR, also in the context of collaborative research, is thus important. In order to give researchers directions for navigating the New Silk Road with research data, in this section, we assess the Chinese approach towards the protection of personal data from the GDPR's perspective.

However, before analyzing the implications of the GDPR's regime on the transfer of personal data for a transfer of personal data to China, it is important to mention that—like De Hert and Papakonstantinou also described in their 2015 report—a system of data protection cannot and should not be broken down to its constitutional parts. Such an approach cannot be used to find common grounds, as one component does not function without the others (De Hert and Papakonstantinou 2015, pp. 13–14). Although the Chinese regime for the protection of personal data as described above is certainly strengthening and becoming more coherent, especially on the internet, such a principle-based system is not in place for the protection of personal data in other spheres. Moreover, a data protection authority does not exist, thereby leaving it up to the individual to enforce his or her data protection rights, which might be very complicated given the individual's relatively weak position before Chinese courts. The GDPR

offers possibilities to compensate for these deficiencies—for example, with legally binding and enforceable instruments between public authorities or bodies, or codes of conduct—but then it is very important to ensure that these instruments can stand the test of the GDPR. In the Chinese context, as described above, where government surveillance rises at the expense of individual privacy and where the power of state authorities is not or only minimally circumscribed by the rule of law, we are not sure to what extent the current discrepancies between the legal systems of the European Union and China can easily be bridged. After all, the seemingly unlimited authority of the American security services to access personal data also was the reason for stopping the exchange of personal data after the *Schrems* case that was also discussed in the "Ensuring a sufficient level of protection" section.

Although we pay heed to the fact that De Hert and Papakonstantinou (2015, p. 28) propagate a pragmatic approach when it comes to sharing personal data with China, we also think it is important to stress that their report seems to be mainly focused on the commercial and economic interests that are served with data sharing. It is true that with regard to such data, a flexible approach might be possible as they are mostly processed via networks and therefore were already covered by legislation such as the aforementioned 2012 decision of the Standing Committee of the National People's Congress on Strengthening Internet Information Protection (see also the section "A brief comparative glance at the Chinese regime for data protection") and currently also by the Cyber Security Law. Research data, however, are not necessarily covered by this legal framework, which seems to be essentially aimed at stimulating public trust and promoting sales, and not so much at providing an individual control over his or her personal information (De Hert and Papakonstantinou 2015, p. 28). Although further arrangements might indeed be able to compensate for this lack of rights and would therefore allow a more pragmatic approach as far as processing of personal data *is* covered by this legislative framework, it is important to make sure that such arrangements are immune to unwarranted government interference. In the current situation, it seems challenging at minimum to meet this requirement. For data that do not fall under the current comprehensive Chinese legislation or special categories of personal data, even more carefulness is deemed to be necessary.

Until clear and more coordinated arrangements—similar to, for example, the EU-US Privacy Shield—have been set up, a safer but also more complicated and fragile option seems to be offered by Art. 49(1) GDPR. Under this provision, a transfer of personal data is also possible in case the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequate decision and appropriate safeguards. Here again, it is important that consent must be given freely (in this regard, see also the section "Ensuring a sufficient level of protection"). Sufficient safeguards therefore need to be provided in order to make sure that a data subject not only consents to the data transfer because it offers him or her access to, for example, experimental treatment. Additionally, arrangements should be made in order to be sure that in such cases, the recognized ethical standards for scientific research that a research object can expect in the European Union are also upheld in China (see for more on this topic, for example, Warrell et al. 2009; Zeng and Resnik 2010; Liu et al. 2015). Finally, there might be cases in which a research institution has compelling interests that necessitate the non-repetitive transfer of the personal data of a limited number of data subjects. Such a transfer is allowed under Art. 49(1) last section GDPR in case it is surrounded with suitable safeguards and the supervisory authority is informed. Given the aforementioned position of research as seemingly subordinate to broader societal goals and as an instrument in government policy strategies (D'Hooge et al.

2018, pp. 11, 25), we deem it hard to provide for such suitable safeguards without having both broader and stronger legal protection in place.

Conclusion

In the European Union, the GDPR regulates the processing of personal data. This legal instrument is applicable to virtually any use of information that can either directly or indirectly be traced back to an individual, and therefore also to information relating to living individuals that is being processed for research purposes. As a form of processing, the transfer of personal data to China in the context of a scientific research has to take place in accordance with the processing principles of the GDPR, meaning that they should be processed in a lawful, fair, and transparent way. Scientific research often concerns sensitive data, such as information on genetics, biometrics, ethnicity, or health. These special categories of personal data may in principle not be processed, unless one of the exceptions mentioned in the GDPR is applicable. Moreover, all personal data should be processed in line with the recognized ethical standards for scientific research, also if they are transferred to a third country. Depending on the policy of the institution to which personal data are being transferred, this might thus necessitate further arrangements in order to make sure that these standards are upheld. Furthermore, the processing may not entail more data than those necessary for the purpose for which they have been collected. On top of that, they should be accurate and not stored for longer than necessary for the scientific purposes that they had been collected for. Lastly, the security of the system used to process the personal data has to be safeguarded.

When the aforementioned conditions have been met, it is to be determined whether the level of protection that is offered by the European Union is not undermined with the transfer of the personal data to China. In determining whether this is the case, not only the specific data protection rules in China should be taken into account but also the system of which these rules form a part. Although we see an increasingly coherent regime in China for the protection of personal data, especially on the internet on the basis of the Cyber Security Law and its further implementation, we have also identified challenges and worrying developments. These include among others a turn away from the rule of law, relatively weak protection of fundamental rights, absence of an independent data protection authority, and an increase of state surveillance. At the same time, we see that academic collaboration with China offers unique opportunities. Also in this field, however, it is important to note that research in China seems to serve broader society and government goals which may lead to individual interests being put aside in order to serve the general interest. From the European perspective on the protection of personal data, such developments are problematic. As long as this can be compensated for by setting up arrangements between the different parties involved, in a way that is immune to unwarranted state interference, a transfer is still possible. However, we question whether such arrangements are realistic in the given situation and we therefore argue that a more comprehensive instrument, for example, similar to the EU-US Privacy Shield, should be set up in order to further facilitate the often indispensable exchange of information and thereby allow science to come to its full potential. In our view, before such rules are established, a great deal of water will have to flow under the newly created New Silk Road bridge. Until then, from the perspective of protecting personal data, the safer way to go is to anonymize personal data that are being transferred to China or to acquire explicit consent of the data subject, after having informed him or her of the risks relating to such a transfer.

Acknowledgments The authors would like to thank Stefan Kulk, Mistale Taylor, Chao Jing, Qiao Cong-rui, Tom Zwart, and Charlotte Mol for their useful comments on earlier versions of this contribution.

References

Article 29 Data Protection Working Party (2007), The concept of personal data (opinion 4/2007). Resource document: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. Accessed 25 Feb 2019.

Article 29 Data Protection Working Party (2010), The concepts of "controller" and "processor" (opinion 1/2010). Resource document: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf. Accessed 25 Feb 2019.

Article 29 Data Protection Working Party (2014), Anonymisation techniques (opinion 05/2014). Resource document: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Accessed 25 Feb 2019.

Barnard, C., & Peers, S. (2014). *European Union law*. Oxford: Oxford University Press.

Buttarelli, G. (2016), The impact of GDPR on collaborative science (speech by Giovanni Buttarelli, EDPS, in seminar organised by ISC Intelligence in Science, Brussels). Resource document: https://edps.europa.eu/press-publications/press-news/videos/impact-gdpr-collaborative-science_en. Accessed 25 Feb 2019.

Chen, H., Chan, B., and Joly, Y. (2015), Privacy and biobanking in China: a case of policy in transition, *Journal of Law*, Medicine and Ethics 4(43), 726–742.

Chen, Y., & Cheung, A. (2017). The transparent self under big data profiling: privacy and Chinese legislation on the social credit system. *Journal of Comparative Law, 12*(2), 356–378.

Deeks, R. (2018), The digital silk road – China's $200 billion project (science focus). Resource document: https://www.sciencefocus.com/future-technology/the-digital-silk-road-chinas-200-billion-project/. Accessed 25 Feb 2019.

D'Hooge, I., Montulet, A., Wolff, M. de, and Pieke, F.N. (2018), Assessing Europe-China collaboration in higher education and research (Leiden Asia Centre), Resource document: http://leidenasiacentre.en/wp-content/uploads/2018/11/LeidenAsiaCentre-Report-Assessing-Europe-China-Collaboration-in-Higher-Education-and-Research.pdf. Accessed 25 Feb 2019.

DG Internal Policies (2016), Data saves lives: the impact of the data protection regulation on personal data use in cancer research – study for the ENVI Committee. Resource document: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/569992/IPOL_STU(2016)569992_EN.pdf/. Accessed 25 Feb 2019.

Dong, M. (2017), China In: A.C. Raul (Ed.), Privacy, data protection and cybersecurity law review. London: Law Business Research.

Economist (2017). China invents the digital totalitarian state. Resource document: https://www.economist.com/briefing/2016/12/17/china-invents-the-digital-totalitarian-state. Accessed 25 Feb 2019.

Economist (2018), China talks of building a "digital silk road". Resource document: https://www.economist.com/china/2018/05/31/china-talks-of-building-a-digital-silk-road. Accessed 25 Feb 2019.

Economist (2019a). How China could dominate science. Resource document: https://www.economist.com/leaders/2019/01/12/how-china-could-dominate-science. Accessed 25 Feb 2019.

Economist (2019b). Can China become a scientific superpower?. Resource document: https://www.economist.com/science-and-technology/2019/01/12/can-china-become-a-scientific-superpower. Accessed 25 Feb 2019.

ECtHR (2018), Guide on Article 8 of the European Convention on Human Rights. Resource document: https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf. Accessed 25 Feb 2019.

EU Delegation to China and Mongolia (2014. Research, innovation and science: cooperation between EU Member States, associated countries, the European Union and China. A testimony of excellence. Resource document: http://eeas.europa.eu/archives/delegations/china/documents/eu_china/research_innovation/6_eumembers_states/140714_eu_ms_and_china_cooperation_brochure_final.pdf. Accessed 25 Feb 2019.

European Commission (2010). Communication from the commission to the European Parliament, the council, the economic and social committee and the committee of the regions: a comprehensive approach on personal data protection in the European Union (COM(2010) 609 final). Resource document: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0609&from=EN. Accessed 25 Feb 2019.

European Commission (2017), Communication from the commission to the European Parliament and the council: exchanging and protecting personal data in a globalised world (COM(2017) 7 final). Resource document: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN. Accessed 25 Feb 2019.

European Parliament (2016), Personal data transfers to China. Resource document: http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/583836/EPRS_ATA(2016)583836_EN.pdf. Accessed 25 Feb 2019.

European Parliament debate (2016), Personal data transfers to China. Resource document: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20160707+ITEM-014+DOC+XML+V0//EN&language=EN. Accessed 25 Feb 2019.

FRA, ECtHR, CoE, EDPS. (2018). *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union.

Glenn, P. (2014), Legal traditions of the *world*. Oxford: Oxford University Press 2014.

Greenleaf, G. (2014). *Asian data privacy laws: trade & human rights perspectives*. Oxford: Oxford University Press.

Greenleaf, G. (2017a). China's new cybersecurity law – also a data privacy law? *Privacy Laws & Business International Report, 144*, 1–7.

Greenleaf, G. (2017b). 2014-2017 update to Graham Greenleaf's Asia data privacy laws – trade and human rights perspectives. *UNSW Law Research Paper, 47*.

De Hert, P. and Papankonstantinou, V. (2015), The data protection regime in China – in depth analysis for the LIBE Committee. Resource document: http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA%282015%29536472_EN.pdf. Accessed 25 Feb 2019.

Hille, C., (22 October 2018), Chinese military researchers exploit western universities (Financial Times), Resource document: https://www.ft.com/content/ebe95b76-d8cc-11e8-a854-33d6f82e62f8. Accessed 25 Feb 2019.

Kirby, W. & Van der Wende, M.(2019), The New Silk Road: implications for higher education in China and the west? *Cambridge Journal of Regions*, *Economy and Society* 12(1). Resource document: https://doi.org/10.1093/cjres/rsy034 .

Kokott, J., & Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law, 4*(3), 222–228.

Li, B. and Wang, J. (2018). China issues personal information security specification. Resource document: https://www.dataprotectionreport.com/2018/02/china-issues-personal-information-security-specification/. Accessed 25 Feb 2019.

Liu, C., Campbell, N., Gerstner, E., Lin, A, Li, P., Pincock, S., Gibbons, C., Zhou, Y., Gilloch, C., Huang, K. and Phillips, N. (2015), *Turning point. Chinese science in transition* (nature publishing group). Resource document: https://www.nature.com/press_releases/turning_point.pdf. Accessed 25 Feb 2019.

Livingston, S., & Greenleaf, G. (2015). The emergence of tort liability for online privacy violations in China. *Privacy Laws & Business International Report, 135*, 22–24.

Maisog, M. and Li, J. (2017), *China* In: A. Bapat and A. P. Simpson (eds.), Data protection, London: Global Legal Group.

McCuaig-Johnston, M. and Zhang, M. (2015), China embarks on major changes in science and technology. *China Institute University of Alberty Occasional Paper Series* 2(2). Resource document: https://cloudfront.ualberta.ca/-/media/china/media-gallery/research/occasional-papers/stmccuaigjohnston-zhang201506.pdf. Accessed 25 Feb 2019.

Narayanan, A. and Shmatikov, V. (2008), Robust de-anonymization of large sparse datasets (2008 IEEE Symposium on Security and Privacy, Oakland).

Nicholson, C. (2018), Data-law mess hampers R&D collaborations (research research). Resource document: https://www.leru.org/files/News/RE-data-law-mess-hampers-rd-collaborations.pdf. Accessed 25 Feb 2019.

Ning, S., & Wu, H. (2018). China. In T. Hickman & D. Gabel (Eds.), *Data protection 2018*. London: ICLG.

OECD (2019a). Gross domestic spending on R&D (China, EU and USA statistics on 28-1-2019). Resource document https://data.oecd.org/chart/5snO. Accessed 25 Feb 2019.

OECD (2019b), R&D intensity in OECD countries and other economies (China, EU and USA statistics on 28-1-2019). Resource document: https://public.tableau.com/shared/H2M9MQYPC?:display_count=no. Accessed 25 Feb 2019.

Normille, D. (2018), China asserts firm grip on research data (ScienceMag). Resource document http://www.sciencemag.org/news/2018/04/china-asserts-firm-grip-research-data. Accessed 25 Feb 2019.

Robinson, N., Graux, H., Botterman, M., & Valeri, L. (2009). Review of the European data protection directive. *Santa Monica: RAND Corporation, 2009* https://www.rand.org/pubs/technical_reports/TR710.html. Accessed 25 Feb 2019.

Sacks, S. (2018a), New China data privacy standard looks more far-reaching than GDPR (Center for Strategic and International Studies). Resource document: https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr. Accessed 25 Feb 2019.

Sacks, S. (2018b), China's emerging data privacy system and GDPR (Center for Strategic and International Studies). Resource document: https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr. Accessed 25 Feb 2019.

Sacks, S., Triolo, P., Webster, G. (2017), Beyond the worst-case assumptions on China's cybersecurity law (new America). Resource document: https://www.newamerica.org/cybersecurity-initiative/blog/beyond-worst-case-assumptions-chinas-cybersecurity-law/. Accessed 25 Feb 2019.

Sacks, S. and Triolo, P., (2017), Shrinking anonymity in Chinese cyberspace (Center for Strategic and International Studies). Resource document: https://www.csis.org/analysis/shrinking-anonymity-chinese-cyberspace. Accessed 25 Feb 2019.

Science Europe (2016), Implications of the GDPR on science and research (presentation by Marie Timmermann). Resource document: http://iscintelligence.com/archivos_subidos/se_implications_of_dpr_on_science.pdf. Accessed 25 Feb 2019.

Sharma, Y. (2018), New data red tape could hamper international research (University World News) Resource document: http://www.universityworldnews.com/article.php?story=20180720072113906. Accessed 25 Feb 2019.

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR)*. Berlin/ Heidelberg: Springer.

Warrell, D. et al (2009), China – UK research ethics (CURE) committee report. Resource document: https://mrc.ukri.org/publications/browse/china-uk-research-ethics-cure-committee-report. Accessed 25 Feb 2019.

Van der Wende, M. and Tijssen, R. (2019), China's belt and road initiative finds new research partners in Europe (nature index). Resource document: https://www.natureindex.com/news-blog/chinas-belt-and-road-initiative-finds-new-research-partners-in-europe. Accessed 25 Feb 2019.

Xia, S. (2017), China cybersecurity and data protection laws: change is coming (China Law Blog). Resource document: https://www.chinalawblog.com/2017/05/china-cybersecurity-and-data-protection-laws-change-is-coming.html. Accessed 25 Feb 2019.

Zeng, W., & Resnik, D. (2010). Research integrity in China: problems and prospects. *Bioethics, 10*(3), 164–171.