12

A European Compass for Transporting Personal Data on the New Silk Road

Stijn van Deursen and Henk Kummeling

12.1 Introduction

In the new era of Open Science, the European Union strongly promotes that all sorts of data should be able to roam freely within the academic world (LERU 2018). A free flow of data enables researchers to not only check and verify each other's work—and thereby to enhance the quality of their work—but also to set up (international) collaborations in which multiple institutions and research communities can benefit from the same data sets. Moreover, data are a key asset in setting up successful research collaborations: not only are they the fuel and catalyst of innovative research, but the sharing of data is also a sign of mutual confidence and respect (Buttarelli 2016). Sharing of data can thereby play a crucial role in scientific advancements.

In light of the rise of Chinese universities, and under influence of the more prominent international positioning of China under the New Silk Road Initiative, Sino–European collaborations in higher education and research are high on the agenda of universities on both ends of the New Silk Road. In all such collaborations, sharing of data will be important.

Yet, the sharing of data might also come with risks, especially when the collaborating universities are rooted in different academic and legal backgrounds. Such risks may be strategic, for example when it comes to sharing military research data. Risks can also relate to the protection of fundamental rights, such as might be the case when data relate to people's private lives. In this contribution, we focus on the latter. In education collaborations, such data may be information about students and staff participating in exchange programs. In research collaborations, such information will mostly relate to researchers and participants to research projects. From the perspective of the European data protection rules, we investigate to what extent personal data can be shared with China. Although the European conditions for sharing of personal data are strict and might pose serious roadblocks on the New Silk Road, we also explore some practical solutions for navigating around such obstacles. This approach is based on the premise that the answer to the question of how much collaboration is possible should be based on a clear strategy, which balances the risks,

Stijn van Deursen and Henk Kummeling, *A European Compass for Transporting Personal Data on the New Silk Road* In: *China and Europe on the New Silk Road: Connecting Universities Across Eurasia*. Edited by: Marijk van der Wende, William C. Kirby, Nian Cai Liu, and Simon Marginson, Oxford University Press (2020).
DOI: 10.1093/oso/9780198853022.003.0012

challenges, and benefits that are involved (d'Hooghe et al. 2018).[1] In order to do so, we begin with providing a general introduction into the European legislation with regard to the protection of personal data and its implications for international collaboration. Our focus then shifts to the regime for the protection of such data in China, after which we identify some difficulties one might come across when transporting personal data on the New Silk Road. We do not carry out a full-fledged, detailed, comparative research, because our initial findings already give a clear direction towards the challenges that have to be overcome. Given these challenges, we subsequently try to provide some directions for navigating on the New Silk Road. Some of the challenges are fundamental and therefore require fundamental legal solutions. Others could probably be dealt with by turning to more technological solutions that can be relied upon to facilitate collaborations, while complying with data protection standards.

12.2 The Protection of Personal Data in the European Union

Personal data is any information that *is* or *can be* related to an identified or identifiable living person (Art. 4(1) General Data Protection Regulation, hereinafter: GDPR).[2] In other words: all information that can be used to identify a person is considered personal data. In the European Union, the protection of such data is a fundamental right, which is enshrined in inter alia the European Charter of Fundamental Rights (Art. 8(1)); the Treaty on the Functioning of the European Union (Art. 16(1)); and the European Convention of Human Rights (Art. 8).[3] This protection does not mean that personal data may not processed, but it does entail that such processing has to take place according to the processing principles that are laid down in the GDPR, which has been in force since May 2018. The main aim of the GDPR is to ensure a consistent and high-level protection of natural persons while facilitating a free flow of personal data (Recital 10 GDPR). In order to do so, the regulation lays down rules for the processing of personal data, and provides individuals whose data are being processed with legally enforceable rights. On top of that, Member State's data protection authorities have to oversee compliance

[1] See further on this topic: *Economist* 2019. See in this light also the recent China strategy of the Dutch government, stating that the Dutch government aims to continue Sino–Dutch collaboration in higher education and research, and trusts that the parties involved will find a balance between the opportunities and risks—especially with regard to unwarranted transfer of amongst others data and while guaranteeing academic freedom (Dutch Ministry of Foreign Affairs 2019, p. 87).

[2] 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.

[3] Here, the right to the protection of personal data is considered to be an aspect of the right to private and family life. See further on the role of this article in the protection of personal data: Council of Europe 2019, p. 35.

with the GDPR's regime.[4] As a regulation, the GDPR is directly applicable in all EU Member States.[5]

The GDPR applies to the *processing* of personal data. Processing is defined in Art. 4(2) GDPR as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." The concepts of personal data, as well as that of processing, are defined broadly, which provides the GDPR with a broad scope of application. Recital 159 GDPR explicitly states that the regulation also applies to the processing of personal data for scientific research purposes.[6] As a result, in cases where research entails the use of data that can be either directly or indirectly related to individuals, such practices are regulated by the GDPR (see also Chassang 2017).

The *controller* is responsible for compliance with the GDPR (Art. 5(2)). The controller is the party that determines the purposes and the means of the personal data processing (Art. 4(7) GDPR). Although researchers are generally free to determine the aims of their research, they usually do so within the limits set by their appointment at a university or another research institute. As a result, the university or research institute will generally qualify as the controller. This conclusion is in line with a 2010-opinion of the Article 29 Data Protection Working Party that preference should be given to consider a company as controller, rather than a specific person within that company. This is to provide data subjects with a stable and reliable entity for the enforcement of their rights (Article 29 Data Protection Working Party 2010). The GDPR applies if the university is established within the EU, or in case the processing activities relate to the monitoring of people's behavior within the EU (Art. 3 GDPR). A further specification of the latter ground for applicability is provided in the European Data Protection Board's Guidelines on the Territorial Scope of the GDPR (2018, pp. 19–20).

In conclusion, almost all sorts of processing of information that can be related to an individual, by a university established within the EU or with regard to the monitoring of the behavior of people within the EU, are covered by the GDPR. When processing such data, the GDPR provisions need to be taken into account: not only is the protection of personal data a fundamental right, which therefore requires careful consideration, but the GDPR also applies a strict sanctioning regime for breaches of its provisions. For example, according to Art. 83 GDPR—depending on the circumstances of a case—the transfer of personal data to China (or to any

[4] See for a more extensive description of the supervisory authority's tasks Art. 57 GDPR.

[5] Art. 288 Treaty on the Functioning of the European Union. However, on some points the EU leaves room for further implementation on a Member State level. See for example Art. 89 GDPR, with references to national law.

[6] Recital 159 furthermore provides that such processing should also be interpreted in a broad manner. It includes for example technological development and demonstration, fundamental research, applied research and privately funded research.

other third country) in breach of the GDPR may result in a fine of €20,000,000. In the following section, we further delve into the GDPR's provisions for such transfers of personal data.

12.3 Transferring Personal Data to a Third Country Under the GDPR

As a form of processing, the transfer of personal data to a country that is not a Member State of the European Union—such as China—should be done in accordance with the GDPR's data processing principles.[7] On top of that, a third country transfer has to comply with specific safeguards.

12.3.1 General Principles for the Processing of Personal Data

The processing of personal data has to take place in line with the six data processing principles that are laid down in Art. 5(1) GDPR. In the following section, we briefly introduce these principles.[8]

Under Art. 5(1)(a) GDPR, personal data firstly have to be processed in a lawful, fair, and transparent way.[9] Grounds for lawful processing are laid down in Art. 6 GDPR. If personal data are processed for administrative or HR purposes, for example for the registration of students or researchers, this processing is likely to take place on contractual basis and can therefore in principle be considered to be lawful.[10] The same applies to processing of data relating to research subjects if this takes place on the basis of their freely given consent.[11] Moreover, such processing is also lawful if this is necessary for either the performance of a task carried out in the public interest, or for legitimate interests pursued by the controller, as long as these interests are not overridden by the interests or fundamental rights and freedoms of the data subject (Art. 6(1)(e) and (f) GDPR). Such interests might for example be relevant in cases of medical research, but still require a careful balancing act to be made.[12]

Furthermore, personal data have to be collected for specified, explicit, and legitimate purposes and may not be processed further than what is necessary for

[7] See also Case C-362/14 *Maximillian Schrems v Data Protection Commissioner and Digital Rights Ireland Ltd* ECLI:EU:C:2015:650, para 45.

[8] See for a more extensive discussion of these principles, also Van Deursen and Kummeling 2019.

[9] The principles of lawfulness, fairness, and transparency.

[10] See Art. 6(1)(b) GDPR.

[11] Art. 6(1)(a) GDPR and Recitals 42–43 GDPR. See for potential complications in acquiring consent: Timmerman, 2016. There is a special regime for consent in medical cases under Regulation (EU) No 536/2014. See also Recital 161 GDPR. See for a further discussion of consent in medical research: Rumboldt and Pierscionek 2017, p. 2.

[12] See on this topic further Van Deursen and Kummeling 2019, pp. 917–920; Chassang 2017.

achieving such purposes.[13] However, further processing for research purposes is possible, if—in accordance with Art. 89 GDPR—additional safeguards are in place to protect the data subject's rights and freedoms.[14]

Thirdly, according to the principle of data minimization, personal data shall be adequate, relevant, and limited in relation to the purposes of their processing.[15] The principle of accuracy, fourthly, entails that personal data have to be accurate and kept up to date if necessary.[16] Moreover, under the principle of storage limitation, personal data must be kept in a form which permits identification of data subjects for no longer than what is necessary for the purposes for which the personal data are processed.[17] Here again, data may be kept for longer periods for research purposes, provided that safeguards are taken in order to protect the rights and freedoms of data subjects in accordance with Art. 89(1) GDPR. Finally, adequate security measures must be taken in order to protect the data.[18]

The GDPR applies a stricter regime for special categories of personal data. Under this regime, the processing of such data is in principle prohibited, except if one of the explicit exceptions mentioned in the GDPR applies. Special categories of personal data are not uncommon in scientific research. They are all sorts of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, 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.[19] Under Art. 9(2)(j) GDPR, the prohibition to the processing of special categories of personal data is lifted in case the data are processed for research purposes and if safeguards are taken to protect the data subject's fundamental rights and interests.[20] Moreover, processing of special categories of personal data is also possible if the data subject has explicitly given his or her consent.[21]

12.3.2 Specfic Requirements for Third Country Data Transfers

The transfer of personal data to a country which is not an EU Member State is only allowed if such transfer does not undermine the European level of protection of the data. Under the regime laid down in Art. 44 and further, the GDPR provides three possible grounds for making sure that the GDPR's level of protection is upheld in case of a third country transfer (see further European Commission 2017). The GDPR's conditions for such transfers also have to be guaranteed in case of an onward transfer of personal data from that third country to another third country.[22]

[13] Purpose limitation, as laid down in Art. 5(1)(b) GDPR. See also: Kaye 2012, pp. 421–422. See for the relevance of pseudonymization therein: Mourby et al. 2018.
[14] Art. 5(1)(b) GDPR. [15] Art. 5(1)(c) GDPR. [16] Art. 5(1)(d) GDPR.
[17] Art. 5(1)(e) GDPR. [18] Art. 5(1)(f) GDPR. [19] Art. 9 GDPR.
[20] See also Art. 89(1) GDPR. [21] Art. 9(2)(a) GDPR.
[22] Art. 44 GDPR.

A transfer of personal data is most convenient if an adequacy decision is granted. In such a decision, the European Commission confirms that the data protection regime of the third country in question ensures an adequate level of protection. It follows explicitly from case law of the Court of Justice of the European Union that a level of protection that is *identical* to that of the EU is not required. Rather, the third country must 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, while also taking into account the European Charter of Fundamental Rights.[23] Other factors to be taken into account when assessing a third country's level of protection are, among others, whether the country in question respects—in both law and practice—the rule of law, human rights and freedoms, the existence of enforceable data subject rights, and restrictions for public authorities from accessing the data.[24] Moreover, it has to be considered whether there is an effectively functioning and independent supervisory authority, that is responsible for ensuring and enforcing compliance with the data protection rules, and is entrusted with adequate enforcement powers for doing so.[25] The required level of independence of a supervisory authority entails inter alia that the authorities remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody, and that they should be provided with sufficient financial means for human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks (Stoddart et al. 2016, p. 147; Balthasar 2013).[26] Finally, the European Commission also has to take account of the international, regional, and multilateral commitments of the third country with regard to the protection of personal data.[27]

If no adequacy decision is granted, a transfer is also possible under Art. 46 GDPR, allowing for third country transfers that are subject to appropriate safeguards and under condition that enforceable data subject rights and effective legal remedies for data subjects are available. Such safeguards should also lay down effective legal remedies to make sure that data subjects can obtain effective administrative or judicial redress or claim compensation in case the data processing principles are breached.[28] Art. 46(2) and (3) GDPR list the ways in which such appropriate safeguards may be provided for. Examples of such safeguards are legally binding and enforceable instruments between public authorities or bodies (Art. 46(2)(a) GDPR), approved codes of conduct (Art. 46(2)(e) GDPR) or contractual clauses that are approved by the supervisory authority (Art. 46(3)(a) GDPR).

[23] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner and Digital Rights Ireland Ltd* ECLI:EU:C:2015:650, para. 73–74. See also European Commission, 2017, section 3.1 and Recital 104 GDPR.

[24] Art. 45(2)(a) GDPR. [25] Art. 45(2)(b) GDPR.

[26] For the requirements with regard to the independence of national supervisory authorities, see Art. 52 GDPR, which is a codification of case law of the Court of Justice of the European Union in the cases C-518/07 *Commission v. Germany* ECLI:EU:C:2010:125 (2010); C-614/10 *Commission v. Austria* ECLI:EU:C:2012:631 (2012); C-288/12 *Commission v. Hungary* ECLI:EU:C:2014:237 (2014).

[27] Art. 45(2)(c) GDPR [28] Recital 108 GDPR.

Finally, if no adequacy decision is granted and if structural additional safeguards are also absent, Art. 49 GDPR provides for derogations for specific situations. Under this article, transfers of personal data to a third country are possible if one of the conditions mentioned in the article applies. With regard to transfers to third countries for research purposes, this may for example be allowed if the data subject has explicitly consented to this transfer, after having been informed of the possible risks of such transfers (Art. 49(1)(a) GDPR). If data are transferred for administrative reasons, such transfers might be allowed if that transfer is *necessary* for the performance of a contract between the data subject and the controller (Art. 49(1)(b) GDPR). Transfers between collaborating universities might also be permitted if such is *necessary* for important reasons of public interest as far as such interests are recognized by EU or Member State law (Art. 49(1)(d) and Art. 49(4) GDPR). Under the last section of Art. 49(1) GDPR, a third country transfer that is not covered by one of the foregoing provisions is also allowed if such transfer is necessary for the purposes of compelling legitimate interests, provided that the transfer is non-repetitive and is surrounded with suitable safeguards, while both the supervisory authority as well as the individuals involved are informed about the transfer. For the interpretation of the concept of "compelling legitimate interests," regard should inter alia be had of the legitimate expectations of society for an increase of knowledge.[29]

12.4 Protecting Personal Data in China: a Brief Comparative Glance Through the Lens of the GDPR

The European Commission has not granted an adequacy decision for China.[30] This means that a transfer of personal data can only take place on the basis of the arrangements discussed in the aforementioned Articles 46 or 49 of the GDPR. To determine whether such arrangements are viable in the context of Sino–European collaborations, in this section we provide a brief comparative glance at both the Chinese approach towards the protection of personal data in the academic world, as well as at the context in which such rules may have to be enforced. Before doing so, it is important to acknowledge that the assessment of the level of protection of personal data in a third country is a complex task that cannot be done exhaustively within the limits of this contribution, especially when the third country's system is rooted in a completely different cultural and legal tradition, such as is the case for China (see also De Hert and Papakonstantinou 2015, p. 7; Greenleaf 2017a, p. 3). Furthermore, it is important to pay heed to the fact that values that are reflected in legislation are not necessarily the same, or similar to, values that form the foundation of European

[29] Recital 113.

[30] See for a current overview of adequacy decisions and ongoing talks on this topic with third countries on this topic: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed November 29, 2019).

legislative instruments (Dutch Ministry of Foreign Affairs 2019, p. 48). Finally, it must be stressed that there can be a difference between the law as it is provided in the books and the way in which it works out in practice. For the aforementioned reasons, we do not aim to provide a complete overview of Chinese law and practice with regard to the protection of personal data or to do a fully-fledged comparative legal study. Instead, we use the GDPR as a guideline for evaluating some of the main characteristics of the Chinese approach towards the protection of personal data and the surrounding legal landscape, as far as they are important for personal data transfers for the purposes of academic collaboration.

The Chinese constitution provides a right to privacy of correspondence in Article 40.[31] It is argued, however, that this article mainly entails a right to dignity and therefore not a right to protect the private sphere of the individual (De Hert and Papakonstantinou 2015, pp. 16–17; Maisog and Li 2017, p. 60). Moreover, it is important to mention that Graham Greenleaf has characterized the Chinese constitution as non-justiciable because Chinese courts are not allowed to nullify legal instruments that violate the constitution, nor to enforce its provisions in order to serve individual interests (Greenleaf 2014, p. 196. Also De Hert and Papakonstantinou 2015, p. 16). This raises doubts as to the level of protection that is actually offered by the Chinese constitution to individuals and their personal data. Yet, more specific Chinese legislation seems to offer more assistance for the protection of personal data. First of all, both civil law and criminal law regulate the use of personal data.[32] However, although this legislation requires the protection of personal data, it is not clear how and on the basis of which principles such protection should be provided. Chinese law, however, sets out clearer guidance for the protection of individuals in the online world. Under the *2012 Decision on Strengthening Internet Information Protection* of the National People's Congress' Standing Committee, network service providers are obliged to comply with data protection principles such as legality, legitimacy, and necessity in case they collect or use citizens' individual electronic information. Moreover, this Decision addresses protection measures to be taken by controllers and introduces rights for data subjects. The *Cyber Security Law* further clarifies the fundamental concepts of data protection and introduces data protection principles that bear resemblance to those provided by the GDPR. The *Cyber Security Law* is further clarified in both the *Guideline for Personal Information Protection within Information Systems for Public and Commercial Services* and the *Personal Information Security Specification*. These last two measures are technical guidelines that are argued to be not legally binding, but would still have persuasive effect on

[31] See for an English translation of the Chinese constitution: http://www.npc.gov.cn/englishnpc/Constitution/2007–11/15/content_1372964.htm.

[32] See Art. 253 and 286(1) Criminal Law as well as several provisions of the 1986 General Principles of the Civil Law and the subsequent 2009 Tort Liability Law. Art. 253 Criminal Law is further interpreted in the Interpretation of the Supreme People's Court Supreme People's Procuratorate on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringement (http://www.spp.gov.cn/xwfbh/wsfbt/201705/t20170509_190088.shtml). See for a more detailed discussion: Ning and Wu, 2018, section 1.2; Livingston and Greenleaf 2015, pp. 22–24; Graham Greenleaf 2017a, p. 19.

parties dealing with personal data in an online environment (DLA Piper 2019), although it is still argued that also under the Specification, unclarity with regard to its interpretation remains (Xiaomeng et al. 2018). The protection of the personal data of consumers is regulated further in, amongst others, the *Consumer Rights Protection Law* and the recent *E-Commerce Law*.

All in all, the description above provides a picture of a still fragmented and sector-specific, yet increasingly more encompassing data protection regime. This picture is confirmed by Chao Ching and Tom Zwart, two experts on Chinese law, who claim that the Chinese regime for the protection of personal data is matching the GDPR's requirements to a large extent.[33] They argue that—although the right to privacy as laid down in the Chinese constitution is not enforceable—the personality rights and right to data protection of the *Tort Liability Law* are. At the same time, they state that the Chinese approach towards the protection of personal data still leaves "considerable room for improvement." In this light, they point to a bill for a *Personal Information Protection Law* that is currently pending before the Standing Committee of the National People's Congress. This bill would provide more rules for the protection of both storage and usage of personal data and at the same time offer individuals rights of access, rectification as well as a right to be forgotten. As part of the 13th Legislative Plan of the Standing Committee, with Class 1 status, the proposal should be enacted during the current five-year legislative plan which runs until 2023 (Xiaomeng et al. 2018).[34]

Although the Chinese regime for the protection of personal data is certainly advancing, some major challenges for transfers of personal data for academic collaboration purposes currently still seem to exist in light of the GDPR's requirements. Firstly, under the GDPR, personal data have to be protected from both private and governmental actors in all forms of processing. The Chinese approach however, seems more focused on the protection of individuals in the online environment, thereby raising questions as to how they are protected in the offline world—in which most academic activities are still situated. Furthermore, although Chinese legislation in the field of the protection of personal data is becoming more coherent as a result of the *Cybersecurity Law* and the *Personal Information Security Specification* (Sacks 2018a; Sacks 2018b), there are still gaps in the framework that might lead to unclarity with regard to the protection of personal data. For example, the exact interpretation of the relevant concepts remains debated, whereas fundamental rules with regard to access rights, data quality requirements, sensitive data, and ongoing transfers are absent (Sacks et al. 2017; Sacks 2017b, sec. 2; Greenleaf 2017b, pp. 2–3; Xiaomeng et al. 2018). At the same time, it remains unclear to what extent the

[33] They sent their report to the authors of this contribution on September 25, 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.

[34] For the latest updates, see https://zh.wikisource.org/wiki/User:NPCObserver/13thNPCSCLegislativePlan. (accessed November 29, 2019).

current rules with regard to protecting personal data are also applicable in the public sector (Xiaomeng et al. 2018).

This brings us to a second challenge. While the use of personal data is thus restricted for some forms of processing in the private sector, the Chinese government is entrusted with more and more tools under among others the *Counterterrorism and Cybersecurity Law* for accessing personal data in order to maintain social order and safeguard security (Xiaomeng et al. 2018). In this context it is important to also mention the so-called Social Credit System that is being developed, in which data—including personal data—play a crucial role (Chen and Cheung 2017; *Economist* 2016). Also, the academic world faces increasing government control, as is exemplified by among others Chinese researchers reporting of cameras in classrooms and restrictions on accessing the Internet (d'Hooghe et al. 2018 p. 11).

In such context, for the protection of individuals, it is especially important to be able to rely upon an independent supervising authority in order to make sure that the existing data protection rights are being enforced in practice. Yet, in China supervisors in this field are often closely related to government departments (Ning and Wu 2018; Sacks 2018b; Dong 2018) and can therefore not be considered independent to the extent required by the European rules and case law. On top of that, there is no clear division with regard to jurisdiction between several government departments that are involved in this field. As a result, a great deal of the enforcement of data protection rules seems to depend upon individual's own efforts to start legal proceedings. Chinese courts are however often described as unwelcoming and subject to political instructions, which causes challenges for the protection of the rule of law and individual rights, whereas judgments are often not enforced or do not provide consistent interpretations of the law (Glenn 2014, p. 351; McCuaig-Johnston and Zhang 2015, p. 29; Greenleaf 2017a, p. 18–19; Dong 2018, section VIII). All these elements are crucial for the protection of personal data under the GDPR. Similar concerns are also expressed by the European Parliament in 2016, pointing at threats to the proper protection of personal data in China arising from a lack of democratic conditions and for the respect of human rights, such as independent courts, legal certainty, and adequate means of enforcement (European Parliament 2016).

12.5 Legal Arrangements for Navigating the New Silk Road

As no adequacy decision is granted with regard to China, the question remains whether entities involved in Sino–European collaborative projects, will be able to provide for appropriate safeguards to make sure that the European level of data protection is upheld when personal data are being transferred to China. Especially so, since the European thresholds are high and require inter alia not only means to enforce data protection rights and for effective legal remedies, to obtain administrative or judicial redress and to claim compensation, but also an evaluation of the context in which such rights and principles have to be enforced.

We acknowledge the fact that China is making advancements with regard to the protection of personal data, especially in certain (private) sectors. Yet, on the basis of the available information it currently seems difficult—if not impossible—to provide for adequate safeguards for bridging the fundamental differences between the Chinese and European approaches with regard to the protection of personal data in the academic sector. First of all, in China universities now seem to fall outside the scope of the Chinese data protection rules. In order to make sure that the required adequate safeguards also apply within this sector, the entities involved could agree on codes of conduct or contractual clauses (Arts. 46(2)(e) and 46(3)(a) GDPR), which have to be approved by the relevant data protection authorities. Subsequently, however, even if such arrangements exist, the rights that are contained in them should also be effectively enforceable and compensation for damages should be available. Here, things get even more complicated; currently in China, independent supervisory authorities seem to be absent or lacking clear guidance as to their respective powers and jurisdiction, whereas judicial protection of individuals is still weak.

Moreover, under the GDPR, personal data should be protected from both private and public actors. This can be complicated given China's focus on security and societal interests over the protection of individual rights, and in light of the fact that higher education institutes are often closely affiliated to, and supervised by, the Chinese government (Jiang and Li 2016. See also Chapter 9 by Gao in this volume). Moreover, recent developments show how the Chinese government is also strengthening its control over scientific data, for example by requiring data to be stored in government-sanctioned data centers (Normille 2018; Sharma 2018; see also Chapter 9 by Gao). All these impediments are closely related to China's institutional set-up and to the functioning of its higher education system, and therefore seem much harder to compensate for by inter-institutional arrangements. Hence, they call for more comprehensive instruments for ensuring a free, but sufficiently protected, flow of personal data.[35] Until such solutions have been found, however, pragmatic solutions might help to navigate around some obstacles on the New Silk Road.

12.6 Technological Solutions for Navigating the New Silk Road

In order to ensure compliance with the GDPR in Sino–European research collaboration, it is important to either anonymize all personal data involved, or to make sure that no data leave the EU. Anonymization, however, may be complicated. Firstly, when anonymizing data, it is important to make sure that (re)identification of an individual is impossible (Article 29 Data Protection Working Party 2014). Secondly,

[35] On this topic: EDPS 2019; Greenleaf 2016. See for an example the EU–US Safe harbor decision, which among others explicitly provides that the data on EU citizens cannot be subjected to surveillance operations. For more information:. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.

for some research projects it might be crucial that information can be linked to the individuals involved as such data would lose their meaning for a researcher if they are anonymized. Also, the anonymization of some sorts of information can simply be impossible given the character of the data involved, as is the case, for example, for genomic data (Beyan et al. 2019, p. 98). At the same time, the rise of all sorts of big data analytics applications make it possible to combine various datasets. This leads to an increase of both the amount and quality of information, and results in new ways for identifying individuals on the basis of data sets. All of this makes anonymization more complicated (Torra and Navarro-Arribas 2016). However, the use of new technologies can also be helpful in setting up research collaborations, for example by facilitating data analysis by partner universities, without the data having to leave the EU. In the following, we shortly explore some of the most promising of these possibilities.[36]

When deciding on whether to make use of such solutions e.g., for facilitating research collaboration, it is important to keep in mind that the protection of personal data should always be the starting point. The methods described here can be helpful in complying with the legal obligations and thereby in making collaborations possible, but they should not be used for circumventing or undermining the law. At the same time, it is important to stress that these technological approaches form rather practical solutions for fundamental problems caused by differences in legal systems. As fundamental problems also require fundamental solutions, it remains crucial to search for solutions on higher levels, in order to bridge some of the most important gaps in the legal pavement of the New Silk Road—for example by concluding agreements as mentioned in the preceding section.[37] Finally, the use of the technologies described here is considered a form of data processing in itself, which therefore has to comply with the GDPR's personal data processing principles.

The *Personal Health Train* is developed within the health care sector.[38] This system enables the analysis of distributed data, while keeping the data in their original location. The main concept behind the system is to bring the analysis to the data instead of bringing the data to the analysis. To do so, distributed and federated analytical tasks visit the data source and execute tasks in a safe environment (Beyan et al. 2019, p. 98). The Personal Health Train infrastructure consists of three main components: trains, stations, and tracks. The train carries an analytical task that is provided by the party wanting to use particular data. This task can be a simple query, but also a self-learning algorithm. The analytical task is executed when the train arrives at the station where the needed data are stored. When arriving at a station, the credentials of the train's analytical task are checked, after which it can access the station and carry out the analysis. Upon leaving the station, the output is checked

[36] We made a selection of these technologies on the basis of discussions with experts from Utrecht University's Research Data Management Services department (see: www.uu.nl/rdm), and various researchers involved in international collaborative projects.

[37] For more on the requirements of such agreements, see EDPS, 2019; Greenleaf, 2016.

[38] For more information, see: https://www.dtls.nl/fair-data/personal-health-train/.

for, among other things, direct and indirect references to individuals. Hence, this process also entails a check to make sure the data that leave the station cannot be used to identify an individual, for example by combining various queries. The tracks are formed by the (legal) rules that govern the analytical task, the communication tool and interfaces. This solution can be helpful when multiple data sources have to be analyzed as there is no need for data to be multiplied or transferred, and can therefore also be a useful tool for enabling collaborative projects (Beyan et al. 2019; for practical examples of research projects implementing Personal Health Train approaches Sun et al. 2018; Van Soest et al. 2018).

Bringing the analysis to the data, instead of bringing data to the analysis, is also possible by applying open algorithms for data analysis (OPAL). In order to make this possible, OPAL uses two tracks: a technology track and a governance track. The technology track consists of an open source platform and open algorithms to analyze data sets. By applying a Q&A approach, the data are analyzed and only aggregated statistics are made available to users. The governance track at its turn aims at making sure that (local) norms are followed and that the outcomes are legal, fair, ethical, and transparent.[39] OPAL algorithms are still being developed, but "[i]f proven successful, [they] could be a powerful tool in unlocking private data for social causes" (McKinsey Global Institute 2018, p. 43). Practical examples of OPAL algorithms' potential for research can among others be found in the research of Salah et al. (2019).

Although the technologies described here might be helpful in facilitating international research collaboration, it is also important to note that technology should not be considered a "silver bullet." On the one hand, using technologies enables the collaborating entities to retain more control over their data than is obtained by transferring data altogether, for example, by checking the rules that are executed. On the other hand, algorithmic systems, and even "simple" rule-based algorithmic systems, can become very complex, especially when multiple systems are interacting. Therefore, one might need e.g., other software to check whether and when an analysis is applied, and what the state of the system is when such task is executed (see on this topic among others Larus et al. 2018). Hence, the technologies that are used should allow for checks with regard to what they are doing, and whether they are doing what they are intended to, and such checks should in practice also be executed. This is in order to make sure that no data leaks occur.

At the same time, for the solutions described here to work in practice, major adjustments in the structuring of data sets and surrounding infrastructures are required. For research partners to develop a script that works in practice, it is important to know how data sets are structured. Currently, researchers in many fields of science often use their own approaches to structuring data sets, which necessitates them to accurately describe these structures for facilitating analysis.

[39] See for a more extensive description of OPAL: https://www.opalproject.org/. For similar approaches: http://www.datashield.ac.uk/.

This may take a lot of effort and is time consuming (Nature 2017). In order to let federated analysis systems operate smoothly, it is important to make sure that data sets are interoperable, for example by applying the FAIR data principles. Achieving interoperability is a field-wide undertaking, which requires among other things that data sets are structured similarly, that sufficient metadata are provided about these sets and that controlled vocabularies are applied. Some fields are already doing well in this regard, while others are still lagging (far) behind. In general, it can be said that the fields that most often work with personal data, such as the social and medical sciences frequently still lack controlled vocabularies and metadata schemes. This might be the result of the rather multidisciplinary character of these fields of science (Niedźwiedzka et al. 2009, p. 55). Other fields of science in which controlled vocabularies are more frequently used, such as physics and geosciences, but also sub domains of life sciences, such as systems biology and bioinformatics, could serve as examples on how to develop more unified vocabularies (Richard et al. 2003; Smith and Kumar 2004; Courtot et al. 2011).

Until the required changes have been made, more traditional solutions could be applied in order to facilitate collaborations. Researchers can for example be given access to facilities at the institute where data are being held, where they are given the opportunity to analyze specifically prepared data sets. The data analysis then has to take place on the spot, while physical and legal measures are taken in order to make sure that the data cannot leave the institute's premises. In this regard, it is important to ensure that the physical and legal measures are not window dressing, but do, in practice, safeguard the required level of protection of data. Mere legal measures, such as giving researchers a temporary appointment at a European university without taking complementary measures might, in this regard, be considered insufficient.

12.7 Conclusion: Dead Ends on the New Silk Road?

Academic collaboration on the New Silk Road frequently entails the exchange of data between institutes in the EU and in China. When such data can be related to individuals, and hence qualify as personal data, the protection of such data is considered a fundamental right. Such data are therefore strongly protected within the European Union. They may only leave the EU if the level of protection offered by the EU would not be undermined by that transfer. This is especially important with regard to data that are processed for research purposes, as such data may often be sensitive in nature.

In this contribution we analyzed the Chinese personal data protection framework, in light of the requirements that are set by the European Union. Although we see that the framework for the protection of personal data in China is advancing, there are still considerable gaps with regard to the protection of such data in academic contexts. Such gaps follow, among other things, from a relatively narrow scope of

rules for processing (mostly focused on online transactions), the lack of an independent supervisory authority, and questions with regard to the protection that is offered against government entities, which—at the same time—play an important role at Chinese universities. In a context where legal proceedings may not always be easily accessible for people wanting to enforce their rights, and where personal data are considered an important asset in setting up state surveillance systems, all of this leads us to the conclusion that there are some considerable obstacles on the New Silk Road.

Legal arrangements can be used to provide a basis for transferring small, non-sensitive datasets, for example for registration purposes, as long as adequate safeguards approved by national supervisory authorities are applicable. For many other types of data that are transferred for purposes of academic collaboration, such as bigger data sets or more sensitive data, these legal arrangements do, however, not seem to be realistic under the current circumstances. All the more so, since such safeguards should also make sure that the people involved can enforce their data protection rights and that effective legal remedies—including for obtaining effective administrative or judicial redress—are available. To enable fruitful collaborations and to be able to benefit the innovative results of Sino–European collaborations, clearer and more coordinated agreements between the EU and China seem to be necessary.

As long as such agreements are not in place, many types of data should be either anonymized, or technological solutions should be applied in order to navigate on the New Silk Road while making sure that fundamental rights are protected and preventing high fines. In our contribution, we therefore also explored some technological solutions for bringing the analysis to the data, instead of the other way around. In light of all this, the New Silk Road should maybe not be considered a dead-end street, but it is safe to say that not all traffic is allowed.

References

Article 29 Data Protection Working Party. 2010. *Opinion 1/2010 on the concepts of "controller" and "processor,"* European Union, accessed November 29, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

Article 29 Data Protection Working Party. 2014. *Opinion 05/2014 on Anonymisation Techniques*, European Union, accessed November 29, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

Balthasar, A., 2013. "Complete Independence" of National Data Protection Supervisory Authorities—Second Try: Comments on the Judgment of the CJEU of 16 October 2012, C-614/10 (European Commission v. Austria), with Due Regard to its Previous Judgment of 9 March 2010, C-518/07 (European Commission v. Germany), *Utrecht L. Rev.* 9(3), pp. 26–38.

Beyan, O., A. Choudhury, J. van Soest, O. Kohlbacher, L. Zimmermann, H. Stenzhorn, Md. Rezaul Karim, M. Dumontier, S. Decker, L. Olavo Bonino da Silva Santos, and A. Dekker. 2019. "Distributed Analytics on Sensitive Medical Data: The Personal Health Train," *Data Intelligence* November 2019, accessed November 29, 2019. https://www.mitpressjournals.org/doi/pdfplus/10.1162/dint_a_00032.

Buttarelli, G. 2016. "The impact of GDPR on collaborative science," accessed November29,2019.https://edps.europa.eu/press-publications/press-news/videos/impact-gdpr-collabor.

Chassang, G. 2017. The impact of the EU general data protection regulation on scientific research, *Ecancer Medical Science* 11.

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

Council of Europe, 2019. "Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence," accessed November 29, 2019. https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

Courtot M., N. Juty, C. Knüpfer, D. Waltemath, A. Zhukova, A. Dräger, M. Dumontier, A. Finney, M. Golebiewski, J. Hastings, S. Hoops, S. Keating, D. B. Kell, S. Kerrien, J. Lawson, A. Lister, J. Lu, R. Machne, P. Mendes, M. Pocock, N. Rodriguez, A. Villeger, D. J. Wilkinson, S. Wimalaratne, C. Laibe, M. Hucka, and N. Le Novère. 2011. Controlled vocabularies and semantics in systems biology, *Molecular Systems Biology* 7, pp. 543–556.

Deursen, S. van and H. R. B. M. Kummeling. 2019. The New Silk Road: a bumpy ride for Sino–European collaborative research under the GDPR?, *Higher Education* 78(5), pp. 911–930.

DLA Piper. 2019. "Data Protection Laws of the World: China," accessed November 29, 2019. https://www.dlapiperdataprotection.com/index.html?t=law&c=CN.

Dong, M. 2018. "China". In A.C. Raul (ed) *Privacy, Data Protection and Cybersecurity Law Review*, edited by A.C. Raul. London: Law Business Research.

Dutch Ministry of Foreign Affairs. 2019. "China Strategy," accessed November 29, 2019. https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/05/15/nederland-china-een-nieuwe-balans/190196–01+Beleidsnota+China+LR+3.pdf. English summary available at: https://www.government.nl/binaries/government/documents/policy-notes/2019/05/15/china-strategy-the-netherlands—china-a-new-balance/Summary+China+strategy.pdf.

Economist. 2016. China invents the digital totalitarian state, 12, December, accessed November 29, 2019. https://www.economist.com/briefing/2016/12/17/china-invents-the-digital-totalitarian-state.

Economist. 2019. How China could dominate science, accessed November 29, 2019. https://www.economist.com/leaders/2019/01/12/how-china-could-dominate-science.

EDPS. 2019. "International Agreements," accessed November 29, 2019. https://edps.europa.eu/data-protection/our-work/subjects/international-agreements_en.

European Commission. 2017. Exchanging and Protecting Personal Data in a Globalised World, accessed November 29, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN.

European Data Protection Board. 2018. Guidelines 3/2018 on the territorial scope of the GDPR, accessed November 29, 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf.

European Parliament. 2016. Personal data transfers to China, accessed November 29, 2019. http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/583836/EPRS_ATA(2016)583836_EN.pdf.

Glenn, H. P. 2014. *Legal Traditions of the World*. Oxford: Oxford University Press.

Greenleaf, G. 2014. *Asian Data Privacy Laws: Trade & Human Rights Perspectives*, Oxford: Oxford University Press.

Greenleaf, G. 2016. International Data Privacy Agreements after the GDPR and Schrems, *Privacy Laws & Business International Report* 136, pp. 12–15.

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

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

Hert, P. de and V. Papakonstantinou. 2015. The data protection regime in China In-depth analysis for the LIBE Committee 2015', accessed November 29, 2019. http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf.

d'Hooghe, I., A. Montulet, M. de Wolff, and F. N. Pieke. 2018. Assessing Europe–China collaboration in higher education and research, accessed November 29, 2019. https://leidenasiacentre.nl/wp-content/uploads/2018/11/LeidenAsiaCentre-Report-Assessing-Europe-China-Collaboration-in-Higher-Education-and-Research.pdf.

Jiang, H. and X. Li. 2016. Party Secretaries in Chinese Higher Education Institutions: What Roles Do They Play?, *J. of Intl. Education and Leadership* 6(2), accessed November 29, 2019. https://pdfs.semanticscholar.org/a1db/58c703bdb4c2ea07aabcdd180df117645aff.pdf.

Kaye, J. 2012. The Tension Between Data Sharing and the Protection of Privacy in Genomics Research, *Annual R. of Genomics and Human Genetics* 13, pp. 415–431.

Larus, J., C. Hanking, S. Granum Carson, M. Christen, S. Crafa, O. Grau, C. Kirchner, B. Knowles, A. McGettrick, D. A. Tamburri, and H. Werthner. 2018. When Computers Decide: European Recommendations on Machine-Learned Automated Decision Making, *Informatics Europe & EUACM Report*, accessed November 29, 2019. https://dl.acm.org/citation.cfm?id=3185595.

LERU. 2018. Open Science and its role in universities: a roadmap for cultural change, accessed November 29, 2019. https://www.leru.org/publications/open-science-and-its-role-in-universities-a-roadmap-for-cultural-change#.

Livingston, S. and G. Greenleaf. 2015. The emergence of tort liability for online privacy violations in China, *Privacy Laws & Business Intl. Rep.* 135.

McCuaig-Johnston, M and M. Zhang, 2015. "China Embarks on Major Changes in Science and Technology," China Institute, University of Alberta Occasional Paper Series Volume 2, Issue No. 2. https://www.ualberta.ca/china-institute/media-library/media-gallery/research/occasional-papers/stmccuaigjohnston-zhang201506.pdf

Maisog, M. and J. Li. 2017. "China," In *The International Comparative Legal Guide to: Data Protection 2017*, edited by A. Bapat and A. Simpson. London: Global Legal Group 2017.

McKinsey Global Institute. 2018. Notes from the AI Frontier. Applying AI for social good, accessed November 29, 2019. https://www.mckinsey.com/featured-insights/artificial-intelligence/applying-artificial-intelligence-for-social-good.

Mourby, M., E. Mackey, M. Elliot, H. Gowans, S. E. Wallace, J. Bell, H. Smith, S. Aidinlis, and J. Kaye. 2018. Are "pseudonymised" data always personal data? Implications of the GDPR for administrative data research in the UK, *Computer Law & Security Review* 34(2), pp. 222–233.

Nature. 2017. Data models to GO-FAIR, *Nature Genetics* 49, p. 971.

Niedźwiedzka, B., K. Czabanowska, and R. Śmietana. 2009. Controlled vocabulary in public health. An overview of the achievements to date, *Journal of Public Health* 17, pp. 55–59.

Ning, S. and H. Wu. 2018. "China," In *The ICLG Guide to Data Protection Laws and Regulations*, edited by T. Hickman and D. Gabel, London: Global Legal Group.

Normille, D. 2018. China asserts firm grip on research data, *ScienceMag*, accessed November 29, 2019. http://www.sciencemag.org/news/2018/04/china-asserts-firm-grip-research-data.

Richard, S. M., J. Matti, and D. R. Soller. 2003. Geoscience Terminology Development for the National Geologic Map Database, *U.S. Geological Survey Open-File Report* 03–471, accessed November 29, 2019. https://pubs.usgs.gov/of/2003/of03-471/richard1/index.html.

Rumboldt, J. and B. Pierscionek. 2017. The Effect of the General Data Protection Regulation on Medical Research, *Journal of Medical Internet Research* 19(2).

Sacks, S. 2018a. "New China data privacy standard looks more far-reaching than GDPR," *CSIS*, accessed November 29, 2019. https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr.

Sacks, S. 2018b. China's emerging data privacy system and GDPR', *CSIS*, accessed November 29, 2019. https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr.

Sacks, S., P. Triolo, and G. Webster. 2017. Beyond the Worst-Case Assumptions on China's Cybersecurity Law, *New America*, accessed November 29, 2019. https://www.newamerica.org/cybersecurity-initiative/blog/beyond-worst-case-assumptions-chinas-cybersecurity-law/.

Salah, A. et al. 2019. *Guide to Mobile Data Analytics in Refugee Scenarios*, Berlin: Springer.

Sharma, Y. 2018. New data red tape could hamper international research, *University World News,* accessed November 29, 2019. http://www.universityworldnews.com/article.php?story=20180720072113906.

Smith, B. and A. Kumar. 2004. Controlled vocabularies in bioinformatics: a case study in the gene ontology, *Drug Discovery Today: BIOSILICO* 2(6), pp. 246–252.

Soest, J. van. 2018. "Using the Personal Health Train for Automated and Privacy-Preserving Analytics on Vertically Partitioned Data," In *Building Continents of Knowledge in Oceans of Data: The Future of Co-Created eHealth*, edited by A. Ugon, D. Karlsson, G. O. Klein, and A. Moen, Amsterdam: IOS Press.

Stoddart, J., B. Chan, and Y. Joly. 2016. The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research, *The Journal of Law, Medicine & Ethics* 44(1), pp. 143–155.

Sun, C., L. Ippel, B. Wouters, J. van Soest, A. Malic, O. Adekunle, B. van den Berg, M. Puts, O. Mussmann, A. Koster, C. van der Kallen, D. Townend, A. Dekker, and M. Dumontieret. 2018. Analyzing Partitioned FAIR Health Data Responsibly, accessed November 29, 2019. https://arxiv.org/ftp/arxiv/papers/1812/1812.00991.pdf.

Timmermann, M. 2016. Implications of the GDPR on science and research, 18, October, accessed November 29, 2019. http://iscintelligence.com/archivos_subidos/se_implications_of_dpr_on_science.pdf.

Torra, V. T. and G. Navarro-Arribas. 2016. "Big data privacy and anonymization". In *Privacy and Identity Management: Facing up to Next Steps*, edited by A. Lehmann, D. Whitehouse, S. Fischer-Hübner, C. Fritsch, and L. Raab. Berlin: Springer.

Xiaomeng, L., L. Manyi, and S. Sacks., 2018. What the Facebook Scandal Means in a Land without Facebook: A Look at China's Burgeoning Data Protection Regime, *CSIS*, accessed November 29, 2019. https://www.csis.org/analysis/what-facebook-scandal-means-land-without-facebook-look-chinas-burgeoning-data-protection.