China's specific regulatory framework on data and how it impacts EU-China R&I collaboration

EU Research and Innovation Knowledge Network on China

Edited by: Niels Kaffenberger, Sarah Morgenstern

ISBN: 978-3-949245-09-1

Disclaimer:

© European Union, 2021

The information and views set out in this document do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

Reproduction is authorised provided the source is acknowledged.

Content

1. Preface

1.1 About the EU R&I Knowledge Network on China

The EU-KNOC initiative was launched in July 2020, by the Directorate-General for Research and Innovation of the European Commission and the Strategic Forum for International Cooperation (SFIC) and is implemented by a consortium consisting of DLR Management Agency, Intrasoft, Teamwork, Technopolis and ZSI. EU-KNOC brings together representatives of the EU Member States' Ministries of Science, Technology and Innovation and other relevant ministries who constitute the Core China Group (CCG) and external experts to tackle thematic issues related to R&I policy towards China and to promote a common response.

As input and background information for EU-KNOC several studies are prepared by a research team. These studies aim to provide more in-depth knowledge regarding specific sub-topics within the wider area of STI collaboration with China.

1.2 Scope and Objectives of this Guiding Paper

Particularly in the context of the current political tensions between China, the US and Europe, the challenges for European and Chinese scientific cooperation have strongly increased. Recently passed new laws in China lead to uncertainties on both sides and effect ongoing and future scientific cooperation. A high degree of uncertainty is evident regarding data security, as it becomes an important aspect of global competition and cooperation. It is now more crucial than ever that scientific cooperation and a dialogue between research actors will continue.

Considering the fact that we are entering an era of digital economy where "data is the new oil"[1] it seems more important than ever to keep up to date with new data laws and regulations.

According to the 14th Five-Year Plan (2021 - 2025) for national economic and social development it is a declared objective to embrace the digital era, unlock the potential of big data, build China's strength in cyberspace, accelerate the development of a digital economy, a digital society, and a digital government, and transform the pattern of production, lifestyle, and governance models through digital transformation.[2]

In view of China's increasing R&I innovation output and scientific efforts of the last years and considering a further increase of R&I spending by more than 7% annually in the future, there is no doubt that China plays a significant role as a future cooperation partner.

China is also advancing its ranking in R&D expenditure and achieved in 2020 the 3rd place in R&D-intensive global companies and No. 1 in patents by origin.[3] The R&D intensity has

[1] Originally coined by the British mathematician Clive Robert Humby.

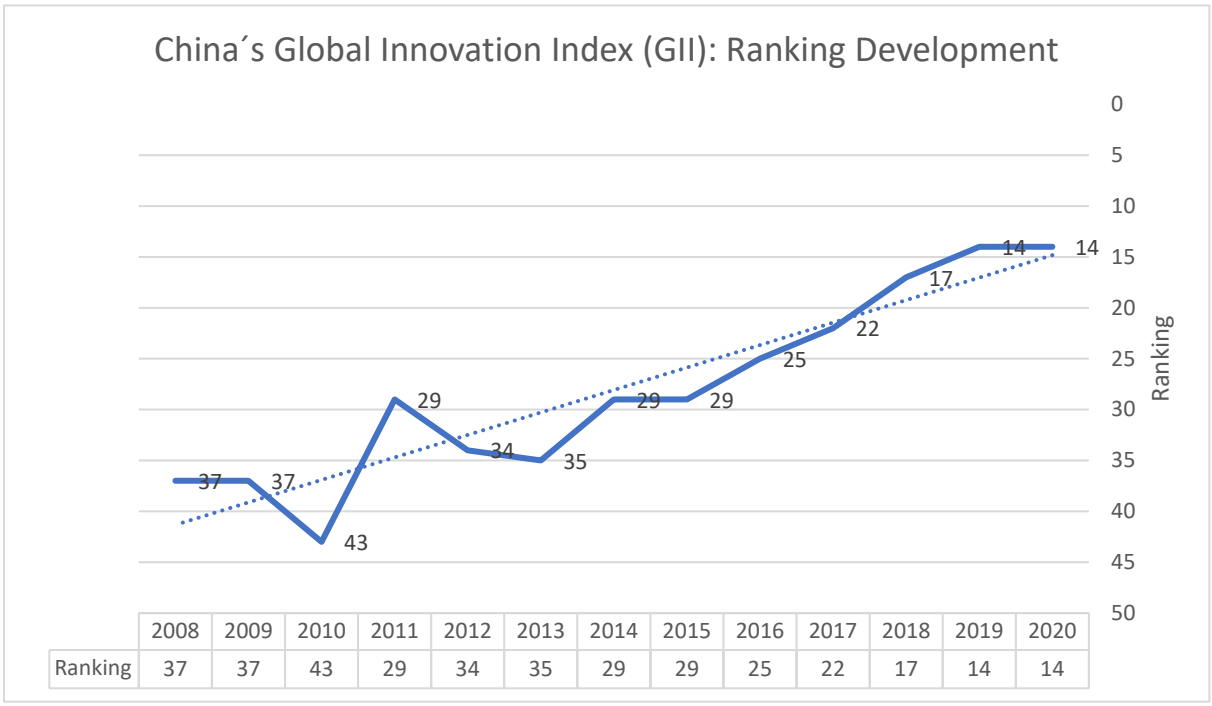
[2] The 14th five-year-plan for national economic and social development of the People's Republic of China and long-range objectives for 2035, 中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要, Zhōnghuá rénmín gònghéguó guómín jīngjì hé shèhuì fāzhǎn dì shísì gè wǔ nián guīhuà hé 2035 nián yuǎnjǐng mùbiāo gāngyào, Part V: Accelerating the digital development, build a digital China, 第五篇加快数字化发展建设数字中国, Dì wǔ piān jiākuài shùzìhuà fāzhǎn jiànshè shùzì zhōngguó. (http://scjss.mofcom.gov.cn/article/zl/zlzc/202103/20210303048609.shtml).

[3] Global Innovation Index 2020, p. 2, 7 (https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2020/cn.pdf).

"skyrocketed" in China and has almost closed the gap with the EU. Moreover, a Chinese company (Huawei) is now in the top three companies worldwide for R&D investment.[4]

On January 27, 2021, the China National Intellectual Property Administration (CNIPA)[5] issued the "Notice on Further Strictly Regulating Patent Application Behavior"[6]. The stated goal of this regulatory document is to improve the quality of patent applications.

A look at China's Global Innovation Index which ranks the innovation capabilities of 131 economies in 2020 emphasises this development:



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Ranking	37	37	43	29	34	35	29	29	25	22	17	14	14

Source: Own figure based on WIPO's GII data[7].

The objective of this paper is to gain an overview of applicable Chinese data laws which are relevant for the research and innovation sectors and to raise awareness for European entities. It will provide a brief description on key elements of China's regulatory framework on data management (including key laws and regulations), that could be challenging for the research and innovation cooperation with China and discuss ways to mitigate possible risks. The laws and regulations introduced in this paper are the Cybersecurity Law of the People's Republic of China (CSL), Export Control Law of the People's Republic of China (ECL), Measures for the Management of Scientific Data (SDM), Data Security Law of the

[4] Grassano, N., Hernandez Guevara, H., Tuebke, A., Amoroso, S., Dosso, M., Georgakaki, A. and Pasimeni, F., The 2020 EU Industrial R&D Investment Scoreboard, p. 33, 53. The other top Chinese R&D relevant companies in 2019 are Alibaba Group Holding, Tencent, China State Construction Engineering (CSCEC) and Baidu.

[5] 国家知识产权局, Guójiā zhīshì chǎnquán jú.

[6] 国家知识产权局关于进一步严格规范专利申请行为的通知, Guójiā zhīshì chǎnquán jú guānyú jìnyībù yángé guīfàn zhuānlì shēnqǐng xíngwéi de tōngzhī (https://www.cnipa.gov.cn/art/2021/1/28/art_75_156439.html), an unofficial English translation is available (https://www.lawinfochina.com/display.aspx?id=34974&lib=law&SearchKeyword=&SearchCKeyword=).

[7] Global Innovation Index 2020: The Global Innovation Index (GII) ranks world economies according to their innovation capabilities consisting of roughly 80 indicators, grouped into innovation inputs and outputs, (https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2020/cn.pdf).

People's Republic of China (DSL) and the Personal Information Protection Law of the People's Republic of China (PIPL).

It is to be expected that the new data laws will affect scientific cooperation between the EU and China in many ways.

The content of this paper is for general information only and is not intended to provide any specific or legal advice or recommendation. The authors explicitly do not accept responsibility or liability in relation to the use of the information. There is no claim for completeness and correctness.

2. Recent legal developments in Chinese data law and challenges for the STI sector

In the last five years the Chinese legislation process regarding data laws and data protection is progressing rapidly.

In China a comprehensive data protection law does not exist.

The General Provisions of the Civil Law of the People's Republic of China[8] stipulate the principle of personal data protection. According to Art. 111 Civil Code the personal information of natural persons shall be protected by law. Any organisation or individual that needs to acquire the personal information of an individual shall obtain such information in accordance with law and guarantee the safety of such information. No one may illegally collect, use, process, transmit, trade, provide or publicise the personal information of others.

Art. 127 Civil Code clarifies if there are laws particularly providing for the protection of data and online virtual assets, such provisions shall be followed.

To understand China's regulatory framework on data it is important to analyse several laws and regulations and to have a general idea of how law is applied in China.

Laws in China have a more holistic approach and are relatively unspecific. Therefore, Chinese laws have to be concretised by specific rules and implementing provisions. Given the vastness of the topic and the unspecific dynamically developing nature of laws, rules and stipulations, the legal framework of data protection is complicated.[9]

China's governance framework on cybersecurity and data security protection is built upon three fundamental[10] regulatory laws: The Cybersecurity Law, the new Data Security Law and the Personal Information Protection Law regulating in China. These are aimed to put limits on data collection and use of sensitive data, ensure data security, and promote an open data policy for data that could have an economic impact.

In comparison to European Union's General Data Protection Regulation (GDPR)[11], the data regulatory in China does not only refer to the personal data area but to a comprehensive

[8] 中华人民共和国民法总则, Zhōnghuá Rénmín Gònghéguó mínfǎ zǒngzé, the English version is published by the National People's Congress, (http://www.npc.gov.cn/englishnpc/lawsoftheprc/202001/c983fc8d3782438fa775a9d67d6e82d8.shtml).
[9] Chen/Han/Kipker, "An Introduction into the New Chinese Data Protection Legal Framework", in: Datenschutz und Datensicherheit - DuD No. 44, (p. 52-57), January 2020, p. 52.
[10] In addition to these fundamental regulations, local regulations may also be taken into consideration.
[11] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

range of data, including state secrets, personal information (including personal sensitive information), important data [12], and other special types of data with industry characteristics.[13]

3. Cybersecurity Law of the People's Republic of China (CSL)

Chinese name:	中华人民共和国网络安全法, Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ[14]
Status of the law:	Entered into force on June 1, 2017
Field of application:	Construction, operation, maintenance, and use of networks, as well as to cybersecurity supervision and management within the mainland territory of the People's Republic of China
Structure:	7 chapters, 79 articles
Specifications:	Specific security protection duties, the "Multi-Level Protection System" (MLPS) have to be complied with
Possible Consequences:	A fine between 10,000 RMB (ca. 1,270 EUR)[15] and 1,000,000 RMB (ca. 12,700 EUR), temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, revocation of business licenses, freezing institutional, organisational, or individual assets or take other necessary punitive measures (see Art. 59 – 75 CSL)

The Cybersecurity Law came into effect on June 1, 2017 and became the first law on a national level to address cybersecurity and data privacy protection in China. The law is divided into seven chapters:

Chapter 1: General provisions

Chapter 2: Support and promotion of cybersecurity

Chapter 3: Network operations security

Chapter 4: Network information security

Chapter 5: Monitoring, early warning, and emergency response

Chapter 6: Legal responsibility

Chapter 7: Supplementary provisions

According to Art. 1 CSL the purpose of the law is to ensure cybersecurity; safeguard cyberspace sovereignty and national security, and social and public interests; protect the

[12] For a more detailed description see p. 15.
[13] Chen/Han/Kipker, p. 53.
[14] An official Chinese version of the CSL is published by the Cyberspace Administration of China (http://www.cac.gov.cn/2016-11/07/c_1119867116.htm), an unofficial English translation is also available (https://digichina.stanford.edu/news/translation-data-security-law-peoples-republic-china).
[15] The average exchange rate from EURO to RMB in 2020 was chosen as the exchange rate. In 2020, 100 Euros received an average of about 787,47 RMB and 1,000 RMB an average of 126,98 EUR.

lawful rights and interests of citizens, legal persons, and other organizations; and promote the healthy development of the informatization of the economy and society.

The law is applicable to the construction, operation, maintenance, and use of networks, as well as to cybersecurity supervision and management within the mainland territory of the People's Republic of China (see Art. 2 CSL).

The broad definition of network users applies in principle to all companies that operate a Chinese internet website, run business operations via Chinese networks or provide online services for customers in China.[16]

Art. 21 CSL outlines the implementation of a cybersecurity **Multi-Level Protection System (MLPS)**[17]. Network operators shall perform the following security protection duties to ensure the network is free from interference, damage, or unauthorized access, and to prevent network data leaks, theft or falsification:

- Formulate an internal security management system and operating rules, determine a person who is responsible for cybersecurity and implement cybersecurity protection responsibility;
- Adopt technical measures to prevent computer viruses, cyber-attacks, network intrusions and other actions endangering cybersecurity;
- Adopt technical measures for monitoring and recording the operational status of the network and cybersecurity incidents and follow provisions to store network logs for at least six months;
- Adopt measures such as data classification, backup of important data[18] and encryption;
- Other obligations provided by law or administrative regulations.

Chapter VI defines the legal responsibility and provides **liability provisions**. Depending on the offence and the relevant circumstances a fine of between 10,000 RMB and 1,000,000 RMB may be levied. The liability could also lead to claims against persons who are directly in charge and other directly responsible personnel. Moreover, temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits or the cancellation of business licenses could be another consequence. In case where foreign institutions, organisations, or individuals are engaged public security departments under the State Council and relevant departments may also decide to freeze institutional, organisational, or individual assets or take other necessary punitive measures (see Art. 75 CSL).

Art. 74 CSL explicitly states that in case that violations of the provisions of the CSL cause harm to others, civil liability and criminal responsibility is borne in accordance with law.

The CSL could affect European R&I entities working on joint research projects with Chinese partners particularly in the field of data processing and data transfers. It is therefore imperative to make sure what kind of data will be processed within the cooperation and where the data are to be stored.

[16] Internal documents provided by Dr. Pattloch/TaylorWessing. Dr. Thomas Pattloch heads the IP department of the China Group at Taylor Wessing and assists European and American companies in all aspects of intellectual property rights in China. In his career, Dr. Pattloch worked for the Asian department of the Max-Planck-Institute, a German law firm in Shanghai and for the EU Commission as the Intellectual Property Officer in the EU Delegation in Beijing.

[17] 网络安全等级保护制度, wǎngluò ānquán děngjí bǎohù zhìdù.

[18] For a more detailed description see p. 14.

In summary, the CSL leads to an administrative burden for the network users and to the obligation to check and monitor the users of relevant platforms like social-media, blogs, or messaging services.[19]

4. Export Control Law of the People's Republic of China (ECL)

Chinese name:	中华人民共和国出口管制法, Zhōnghuá Rénmín Gònghéguó chūkǒu guǎnzhì fǎ[20]
Status of the law:	Entered into force on December 1, 2020
Field of application:	Cross-border and in-country data transfers under relevant export control provisions
Structure:	5 chapters, 49 articles
Specifications:	Extraterritorial application, specific provision for "in-country" transfers
Possible Consequences:	
	• A fine that is greater than five times of and smaller than ten times of the illegal turnover[21] if the gains are more than 500.000 RMB (ca. 63,500 EUR), or a fine between 500,000 and 5,000,000 RMB (ca. 635,000 EUR) if there are no gains made from illegal activities or the illegal turnover is less than 500,000 RMB (e.g. exporting without qualification or approval by SECADs, Art. 33, 34 ECL);
	• A fine that is greater than ten times of and smaller than twenty times of the illegal turnover if the illegal turnover is more than 500,000 RMB or a fine that is greater than 500,000 RMB and smaller than 5,000,000 RMB if there is no illegal turnover or the illegal turnover is less than 500,000 RMB (e.g. export activities with "listed" importers and end-users, Art. 37 ECL);
	• A warning or order that the violation has to be stopped, confiscation of illegal income, business suspension, revocation of export business qualifications and restrictions on the responsible individuals' future involvement in export activities. (see Art. 33 – 44 ECL)

On December 1, 2020 the Export Control Law of the People's Republic of China (the ECL) came into force. Before the law took effect, China's export control was regulated by

[19] Internal documents provided by Dr. Pattloch/TaylorWessing.
[20] An official Chinese version of the ECL is published by the State Council of the People's Republic of China (http://www.gov.cn/xinwen/2020-10/18/content_5552119.htm), an unofficial translation is published by the law firm Covington & Burling LLP (https://www.cov.com/-/media/files/corporate/publications/file_repository/prc_export_control_law_2020_10_cn_en_covington.pdf).
[21] 违法经营额, Wéifǎ jīngyíng é (literally translated "amount of illegal business").

industry-specific measures and lists issued by various ministries.[22] The ECL establishes China's first comprehensive framework for export control. The ECL complements the "Unreliable Entity List System"[23], which targets individuals and organisations and imposes restrictions on them. According to "the Provisions on the Unreliable Entity List", foreign entities (including enterprises, other organisations or individuals of a foreign country), if included in the list, may be prohibited from importing or exporting to or from China as a possible measure.[24]

The ECL is divided into five chapters:

Chapter 1: General provisions

Chapter 2: Control policies, control lists and control measures

Chapter 3: Regulation

Chapter 4: Legal responsibility

Chapter 5: Supplementary provisions

According to Art. 1 and Art. 3 ECL the purpose of the law is to safeguard national security and interests, perform international obligations such as non-proliferation and other, and enhance and regulate export control. Furthermore, a national security perspective that preserves international peace and improves export control administration and services shall be adopted.

Art. 2 and Art. 4 ECL define the material scope of the law. Controlled items include dual-use, military and nuclear items; items relating to the performance of anti-proliferation and other international obligations; other goods, technologies, services[25] and items relating to the maintenance of national security and national interests.

The new law extends the definition of controlled items to **encompass technical information [26] and other data** in connection with listed items (e.g. technical documentation). Research, joint research or technology sales provided as a service by a domestic entity may be considered as technology exports and thus might be controlled. Whether the elements are regarded as controlled items depends on the details of the control lists[27] that are constantly updated (Art. 9 ECL).[28] In addition, to general control lists, the law (Art. 9 ECL) authorises **State Export Control Administrative Departments**

[22] The relevant legal sources can be found in: Joint EU-China Handbook on Export Control of Dual-Use-Items, Vol. 1, Part. II.

[23] MOFCOM Order No. 4 of 2020 on Provisions on the Unreliable Entity List, 商务部令 2020 年第 4 号 不可靠实体清单规定, Shāngwù bù lìng 2020 nián dì 4 hào bù kěkào shítǐ qīngdān guīdìng,
in Chinese: (http://www.mofcom.gov.cn/article/b/fwzl/202009/20200903002593.shtml)
in English: (http://english.mofcom.gov.cn/article/policyrelease/questions/202009/20200903002580.shtml).

[24] See Art. 10 MOFCOM Order No. 4 of 2020 on Provisions on the Unreliable Entity List. Until today there are no recorded entities (15th September 2021).

[25] The law does not differentiate between technologies and services (Höft, "Das neue Exportkontrollgesetz der VR China im Überblick", in ZChinR 2021, p. 27).

[26] 技术资料, Jìshù zīliào.

[27] There are several lists with items that are regulated or temporarily regulated by the provisions of the ECL. Examples are: Two catalogues with items for which an import or export ban exists (http://www.mee.gov.cn/xxgk2018/xxgk/xxgk10/202101/t20210107_816408.html); A catalogue of goods subject to export authorisation: http://www.mofcom.gov.cn/article/b/e/202012/20201203027824.shtml; A catalogue of dual-use items (http://www.mofcom.gov.cn/article/b/c/202012/20201203027833.shtml).

[28] Internal documents provided by Dr. Pattloch/TaylorWessing.

(SECADs)[29] to list items for "temporary controls" for a provisional period up to two years before determining whether to list the items on a control list.

Art. 12 (Catch-all clause) stipulates that non-listed goods can also be subject to export licensing if they pose a threat to national or security interests, can be used in connection with a mass destruction weapon or for terrorist purposes.

According to Art. 4 ECL the state implements a unified export control system, and oversees the system by making control lists, directories, and catalogues, and implementing export licensing.

Controlled entities according to the ECL are:

- Exporters[30] who may be exporting Control List items or items that are temporarily controlled or prohibited (see Art. 11, 12, 13, 39 ECL)
- Service providers (such as agency, shipping, delivery, custom clearance, third-party-ecommerce trading platform services, etc.) who carry out illegal acts in connection with export controls (see Art. 19, 20, 36 ECL)
- Importers and end-users who are listed on the control list for importers and end-users (Art. 18 ECL)

Importers and end-users who are included on the restricted list are prohibited or restricted from deals relating to controlled items, the export of the related controlled items can be suspended, and export licensing facilitation measures can be withheld.

According to Art. 15 and 16 ECL not only end-users but also the end-use of the items is controlled: End-users provide and secure official certificates on the end use and to pledge that no transactions to third parties or repurposing of controlled items will take place. Exporters and importers have to report when detecting any irregularities to SECADs. With this and other provisions (e.g. Art. 17, 18, 44 ECL), the ECL includes extraterritorial jurisdictional and enforcement powers. According to Art. 44 ECL not only Chinese citizens but any organisation or individual outside of the territory of the People's Republic of China that violates the provisions of the law in relation to the administration of export control, endangers the national security and national interests of China and hinders the performance of non-proliferation and other international obligations, shall be subject to investigation and legal liability in accordance with the law.

Controlled activities according to the ECL are:

- General export: Transfer of controlled items out of the People's Republic of China (Art. 2 ECL)
- Activities deemed as export: The provision of any controlled items by any citizens, legal persons or non-corporate organisations of the People's Republic of China to any foreign organisations or individuals (Art. 2 ECL)
- Re-export: Transit, transshipment or re-export[31] of any controlled items (Art. 45 ECL)

[29] 国家出口管制管理部门, Guójiā chūkǒu guǎnzhì guǎnlǐ bùmén.

[30] According to Art. 12 ECL exporters must apply for an export licence from the relevant SECADs, in order to export any item listed on the control lists or subject to temporary controls. Permits are still needed for uncontrolled items when exporters know or should know items may impose national security risks. Licence applications are to be assessed based on: national security and interests, international obligations and commitments, type of export, sensitivity of items, destination country or region, end users and end use, the exporter's credit history; and any other factors to be prescribed by law or regulations (Art. 13 ECL). Exporters are encouraged to establish internal compliance auditing departments (Art. 5 ECL).

[31] The term re-export is not defined in the law.

- Special export: export of any controlled items from bonded areas, export processing zones and other areas specially regulated by the customs and regulated bonded places (Art. 45 ECL)

Indirect export activities such as activities deemed as export and re-export expand the scope and forms of controlled activities. Thus, the in-country transfer of controlled items to foreign entities can be controlled.[32] Art. 2 ECL can be understood in such a way that the transfer of controlled goods outside China to any foreign organisation or individual is also considered as export (deemed re-export). This means, for example, that a permission is also required if a Chinese citizen, residing in the EU, transfers controlled items to a European citizen. In this way, an exchange between Chinese and other nationals in a research and development department of a company may require an approval by the relevant authorities.[33]

Possible sanctions according to the ECL are (e.g.):

- Export without qualification, export of controlled items without approval or beyond the approved scope specified in the export license, export of goods that are prohibited from being exported: the authorities shall issue a warning, order that the violation has to be stopped, confiscate any illegal income, and impose a fine that is greater than five times of and smaller than ten times of the illegal turnover if the gains exceed 500.000 RMB, or a fine between 500,000 and 5,000,000 RMB if there are no gains made from illegal activities or the illegal turnover is less than 500,000 RMB (see. Art. 33/34 ECL).
- In serious cases the export operator shall be ordered to suspend business for rectification and his/her qualification for export to related controlled items may even be revoked (see. Art. 34 ECL).
- Export activities with importers or end-users on the restricted list (Art. 18 ECL): authorities can issue a warning, order the violation to be stopped, confiscate any illegal income and impose a fine that is greater than ten times of and smaller than twenty times of the illegal turnover if the illegal turnover is more than 500,000 RMB or a fine that exceed 500,000 RMB and smaller than 5,000,000 RMB if there is no illegal turnover or the illegal turnover is less than 500,000 RMB (see. Art. 37 ECL).
- Any sanction under these provisions results in SECADs being prohibited from issuing an export license to the sanctioned exporter for a period of five years; any person that is directly responsible for such violation may be prohibited from engaging in relevant export activities for five years, and any person who receives any criminal penalty for any export control violation shall not engage in relevant export activities during his/her lifetime (Art. 39 ECL).

The ECL could affect European R&I entities working on joint research projects with Chinese partners basically in every kind of activity. In this regard it is in particular necessary to become familiar with the respective lists.

In summary, the ECL extends the scope of controlled items to technical information and data. The law covers more controls activities ranging from cross-border movements to in-country transfers. The export control regulations may be changed regularly due to issuing temporary lists for items and the adaption of the Provisions on the Unreliable Entity List, while assigning compliance responsibility to exporters. This ongoing process requires continuous monitoring.

[32] Internal documents provided by Dr. Pattloch/TaylorWessing.

[33] Höft: "Das neue Exportkontrollgesetz der VR China im Überblick", in ZChinR 2021, p. 27-28).

5. Measures for the Management of Scientific Data (SDM)

Chinese name:	科学数据管理办法, kēxué shùjù guǎnlǐ bànfǎ[34]
Status of the law:	Entered into force on March 17, 2018
Field of application:	Any unit or individual engaging in activities related to scientific data supported by Chinese government budget funds
Structure:	6 chapters, 33 articles
Specifications:	Submission of scientific data to relevant "Scientific Data Centers"
Possible Consequences:	Unwanted data loss, sanctions, blacklisting, classification of scientific data, establishment of a scientific data management system

The Measures for the Management of Scientific Data came into effect on March 17, 2018 and focus on the protection of scientific data. It is divided into 6 chapters:

Chapter 1: General provisions

Chapter 2: Responsibilities

Chapter 3: Collection, archiving, and preservation

Chapter 4: Sharing and utilization

Chapter 5: Confidentiality and security

Chapter 6: Supplementary provisions

According to Art. 1 SDM the purpose of the measures is to further strengthen and standardise the management of scientific data, ensure the safety of scientific data, improve the level of open sharing, and better support innovation in national science and technology, economic, social development, and national security.

The measures are applicable to the collection, generation, processing, open sharing, management and usage of scientific data **supported by government budget funds**. Any unit or individual engaging in activities related to scientific data within the People's Republic of China should implement them in accordance with these measures should such activities fall within the conditions stipulated by these measures (see Art. 3 SDM).

The measures could also be applicable to data which were generated outside the territory of the People's Republic of China. This could be the case if the data would be transferred to China by a mechanism which is financed by the Chinese government.[35] It is therefore of high importance to verify the financial background of the Chinese research partner.

According to Art. 13 SDM, all scientific data that are derived from the science and technology plans (special projects, funds, etc.) and financed by government budget funds shall be submitted to the relevant **Scientific Data Centers[36]** by the leading entities of the

[34] An official Chinese version of the SDM is published by the State Council of the People's Republic of China (http://www.gov.cn/zhengce/content/2018-04/02/content_5279272.htm), an unofficial English translation is also available (https://www.enago.com/academy/china-open-science-open-data-manadate-released/).
[35] Internal documents provided by Dr. Pattloch/TaylorWessing.
[36] 科学数据中心, kēxué shùjù zhōngxīn.

projects. Art. 13 SDM also stipulates that all scientific data generated after the acceptance of the project/subject shall also be submitted.

Art. 14 SDM stipulates that the responsible authorities and legal entities shall establish a management system for archiving data regarding domestic and foreign academic papers. When scientific data which were generated with the support of government budget funds have to be submitted overseas for written academic papers and will be published in foreign academic journals using the aforementioned scientific data, the authors shall submit these scientific data to their relevant units for a unified management before the paper is published.

Scientific data concerning state secrets, national security and the public interest generated by social funds must be submitted according to Art. 15 SDM. The submission of other scientific data generated by social funds to the relevant Scientific Data Centers is encouraged. Consequently, this could lead to the submission of trade secrets if the scientific data are state secrets or are related to national security or public interests.[37]

In accordance with Art. 25 SDM scientific data involving state secrets, national security, public interest, trade secrets or personal privacy shall not be made publicly available. If it is required to make the data publicly available, they must be subject to a review of the purposes of use, user qualifications and confidentiality conditions. Furthermore, the scope of the release shall be strictly controlled.

When scientific data is required for government decision making, public safety, national defense construction, environmental protection, disaster prevention and reduction, public welfare research, etc., the legal entities shall provide such data without compensation (see Art. 24 SDM). If a fee is needed, a reasonable standard shall be formulated in accordance with prescribed procedures and the non-profit principle.

Art. 31 SDM also stipulates possible **sanctions** in cases of data forgery, intellectual property rights infringement and submitting data not according to the relevant provisions. The responsible authorities may, according to the severity of the circumstances, punish the relevant entities and responsible persons by ordering them to make corrections, announce criticism, taking disciplinary actions or administrative punishments according to the law. In addition, and in accordance with the national cybersecurity management regulations, Art. 28 SDM contains the possibility of "blacklisting" within a network security system.

According to a statement by the Ministry of Science and Technology of the People's Republic of China (MOST) it is intended to avoid a situation in which scientific data financed by Chinese government budget funds, will be transferred abroad without having archived the data by the relevant Scientific Data Centers beforehand. Nevertheless, the SDM explicitly shall not stop the outgoing flow of scientific data.[38] Moreover, the responsible authorities and legal entities shall actively promote the publication dissemination of scientific data (see Art. 22 SDM).

The SDM could affect European R&I entities working on joint research projects with Chinese partners whenever the cooperation is supported by Chinese government budget funds.

In summary, the major purpose of the SDM is to exert control over Chinese government funded research. To act in accordance with the SDM it is thus necessary to **classify the scientific data** in order to evaluate if they are affected by the relevant provisions, to **clarify the level of confidentiality** (including the confidentiality period) and to **establish**

[37] Internal documents provided by Dr. Pattloch/TaylorWessing.
[38] Internal documents provided by Dr. Pattloch/TaylorWessing.

a scientific data management system (these obligations are also explicitly stated in Art. 20 SDM).

6. Data Security Law of the People's Republic of China (DSL)

Chinese name:	中华人民共和国数据安全法, Zhōnghuá Rénmín Gònghéguó shùjù ānquán fǎ[39]
Status of the law:	Entered into force on September 1, 2021
Field of application:	Processing of data (any record of information in electronic or any other form) even outside the territory of China
Structure:	7 chapters, 55 articles
Specifications:	Extraterritorial application, specific provision for "new technologies"
Possible Consequences:	A fine between 10,000 and 10,000,000 RMB (ca. 1,270 and 12,700 EUR), suspension of services, revocation of the relevant business permission or license, classification of data

The Data Security Law is the statutory basis for data processing within China and provides a further legal basis for the Chinese authorities to enforce data security requirements. For the first time different aspects of data protection and the use of data are combined in one law. The DSL is divided into 7 chapters:

Chapter 1: General provisions

Chapter 2: Data security and development

Chapter 3: Data security system

Chapter 4: Data security protection obligations

Chapter 5: Security and openness of government data

Chapter 6: Legal responsibility

Chapter 7: Supplementary provisions

According to Art. 1 DSL the law is formulated to regulate the processing of data, ensure data security, promote the development and exploitation of data, protect individuals and legitimate rights of organisations and interests, safeguard national sovereignty, security and development interests.

The law is applicable to data processing activities and security supervision carried out within the territory of the People's Republic of China. Data processing activities carried out **outside the territory** of the People's Republic of China that are harming the national security of the People's Republic of China, the public interest, or the legitimate rights and interests of citizens and organisations, are to be pursued for legal responsibility according to the law (see Art. 2 DSL).

[39] The Chinese version is published by the National People's Congress (http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml), an unofficial translation is also available (https://digichina.stanford.edu/news/translation-data-security-law-peoples-republic-china).

The definition "data" according to DSL means any record of information in electronic or any other form (Art. 3 DSL). In addition to digital and cyber information, information recorded in other forms (e.g. hard records of information) is also covered.

The DSL establishes a **data classification** management and protection system. Data are divided into three classes based on the importance of data, namely national core data[40], important data[41], and general data (see Art. 21 DSL). National core data are related to national security, the lifeline of the national economy, important aspects of people's livelihood, major public interests, etc. These data require the implementation of a stricter management system. Additionally, the state conducts national security reviews of data processing activities that impact or might impact national security. The security review decisions are final decisions (see Art. 24 DSL).

In accordance with the graded protection system for data, each region and department shall determine a specific catalog of important data for the respective region, department, or relevant industry and conduct a special protection of data listed in the catalog.

The processor of important data shall periodically conduct risk assessments of such data processing activities and submit risk assessment reports to the relevant department in charge. The risk assessment report shall include the type and quantity of important data being processed, the circumstances of the data processing activities, the data security risks faced and measures to address them (see Art. 30 DSL).

Neither the CSL nor the DSL provides details regarding the definition and scope of **important data** and the detailed protection mechanism. A reference to the definition of important data is provided in other legal documents which have been published only for public comment and are not finalised yet. In May, 2019, the Cyberspace Administration of China ("CAC")[42] released the draft Measures for Data Security Management ("Draft Measures")[43] for public comment. Art. 38 of the draft defines important data as the kind of data, if divulged, may directly affect national security, economic security, social stability, public health and security, such as undisclosed government information, large-scale population, genetic health, geographic, mineral resources. Important data usually does not include information related to the production and operation of enterprises, internal management information or personal information.

The Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Comment), published in August 2017, also provides a definition for important data as the data (including raw data and derived data) collected, generated in China by relevant organisations, institutions, or individuals that are closely related to national security, economic development and public interests, but do not involve national secrets.[44]

Nevertheless, the definition of important data remains vague and broad.

The DSL also implements a cybersecurity **Multi-Level Protection System (MLPS)** in Art. 27 DSL and refers to the CSL (see above).

[40] 国家核心数据, Guójiā héxīn shùjù.

[41] 重要数据, Zhòngyào shùjù.

[42] 国家互联网信息办公室, Guójiā hùliánwǎng xìnxī bàngōngshì.

[43] An official Chinese version of the Draft Measures is published by CAC (http://www.cac.gov.cn/2019-05/28/c_1124546022.htm), an unofficial translation is published by the law firm Covington & Burling LLP (https://www.insideprivacy.com/wp-content/uploads/sites/51/2019/05/Measures-for-Data-Security-Management_Bilingual-1.pdf).

[44] Internal documents provided by Dr. Pattloch/TaylorWessing.

To safeguard national security, national interests and to fulfill international obligations the DSL requires the implementation of export control measures for data to be transferred overseas as controlled items (see Art. 25 DSL).

When any country or region adopts discriminatory prohibitions, restrictions or other similar measures against the People's Republic of China that are relevant to investment or trade in data and technology for the exploitation and development of data, the People's Republic of China may take reciprocal measures against that country or region based on the actual circumstances (see Art. 26 DSL).

Art. 28 DSL contains a specific provision regarding the processing of data in the field of "**new technology**"[45]. These data shall be conducive to promoting economic development, improving the well-being of the people, and complying with public moral and ethics. A definition of "new technology" is not provided. In particular, the term "public moral and ethics" can be interpreted in various ways and a clarification would be highly appreciated in order to avoid any liability according to Art. 2 DSL.[46]

Art. 45 DSL stipulates **penalties** when organisations or individuals conducting data processing activities which do not comply with the data security protection obligations provided in articles 27, 29, and 30 DSL. The responsible departments in charge shall order corrections, give warnings and may also impose a fine between 50,000 and 500,000 RMB and a fine between 10,000 and 100,000 RMB on directly responsible management personnel and other directly responsible personnel. Those who refuse to make corrections or caused violations with serious consequences such as a large-scale data leak are to be fined between 500,000 and 2,000,000 RMB and may be ordered to suspend relevant services, suspend services for rectification or have their relevant business permission or license revoked. Directly responsible management personnel and other directly responsible personnel are to be fined between 50,000 and 200,000 RMB. Whereas, if core national data management systems are violated, relevant departments in charge are to impose a fine of between 2,000,000 and 10,000,000 RMB and according to the circumstances may be ordered to suspend relevant services, suspend services for rectification have their relevant business permission or license revoked.

The DSL could affect European R&I entities working on joint research projects with Chinese partners particularly when processing "national core data", "important data" and data in the field of "new technologies".

In summary, the scope of application covered by the DSL is very broad. To fulfil the requirements, it is necessary, to establish a data security and protection system and security assessment schemes. Particularly, the extraterritorial application is a major aspect which must be considered when processing data. As a consequence, research activities could be sanctioned under this law, if they might harm the national security, the public interest, or the legitimate rights and interests of citizens and organisations of the People's Republic of China.

[45] 新技术, Xīn jìshù.

[46] Internal documents provided by Dr. Pattloch/TaylorWessing.

7. Personal Information Protection Law of the People's Republic of China (PIPL) - Draft

Chinese name:	中华人民共和国个人信息保护法, Zhōnghuá Rénmín Gònghéguó gèrén xìnxī bǎohù fǎ[47]
Status of the law:	Will become effective on November 1, 2021
Field of application:	Processing of personal information of natural persons
Structure:	8 chapters, 74 articles
Specifications:	Comparable with the General Data Protection Regulation (GDPR) in the European Union
Possible Consequences:	Administrative burden, export restrictions of personal information, sanctions (fine of up to 1,000,000 RMB (ca. 127,000 EUR), in serious cases up to 50,000,000 RMB (ca. 6,350,000 EUR) or up to 5% of the annual revenue, suspension of the business, recording in the credit files)

The draft of the PIPL was approved on August 20, 2021 by the Standing Committee of the National People's Congress of the People's Republic of China and is coming into effect in November 1, 2021. The full text has not been made public yet. The draft is divided into 8 chapters:

Chapter 1: General provisions

Chapter 2: Rules on processing of personal information

Chapter 3: Rules on cross-border provision of personal information

Chapter 4: Rights of individuals in processing of personal information

Chapter 5: Obligations of personal information processors

Chapter 6: Authorities fulfilling personal information protection duties and responsibilities

Chapter 7: Legal responsibility

Chapter 8: Supplementary provisions

According to Art. 1 PIPL the law is enacted to protect personal information rights, regulate personal information processing activities and to promote a reasonable use of personal information on the basis of the constitution.

The law was described as "one of the world's toughest on personal data security"[48]. The impact of the law is often compared with the implementation of the **General Data Protection Regulation (GDPR)** in the European Union. Indeed, there are some notable similarities to the GDPR standard.

[47] The Chinese version is published by the National People's Congress (http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml), an unofficial English translation is also available (https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021).

[48] Qu, Tracy, "China's sweeping Personal Information Protection Law to come into effect on November 1", in South China Morning Post (SCMP), August 20, 2021 (https://www.scmp.com/tech/policy/article/3145763/chinas-sweeping-personal-information-protection-law-come-effect).

According to Art. 13 PIPL personal information processors may only process personal information when they conform to one of the following circumstances:

- Where the individual has consented to the processing
- Where the processing is necessary for the conclusion and performance of a contract in which the individual is a party in, or according to labour rules, or to conduct human resources management
- Where the processing is necessary to fulfill legal duties or statutory obligations
- Where the processing is necessary to respond to sudden public health incidents or in emergency circumstances to protect the life, health and the security of the property of natural persons
- Where it is necessary to process personal information within a reasonable scope to implement news reporting, to conduct public opinion supervision, and other such activities in the public interest
- Where it is necessary to process personal information within a reasonable scope when the personal information is disclosed by the person themselves or otherwise already lawfully disclosed
- In other circumstances provided in laws and administrative regulations

Where personal information is processed on individual consent, the consent shall be given voluntarily and explicitly by the individual under the precondition of full knowledge (see Art. 14 PIPL).

The law is not only applicable to the processing of personal information of natural persons within the territory of China but also applies outside China for the purpose of providing goods or services to natural persons in China, analysing and evaluating activities of natural persons in China and other circumstances stipulated by laws and administrative regulations (see Art. 3 PIPL).

The **export of personal information** is subject to specific conditions according to Art. 38, 40 PIPL. It shall meet one of the following conditions:

- Pass the security assessment by the national cyberspace affairs authorities[49] according to Art. 40 PIPL
- Approval by the national cyberspace affairs authorities
- Entering a contract with the overseas recipient in accordance with the standard contract formulated by the national cyberspace affairs authorities
- In accordance with laws, administrative regulations or other conditions provided by the national cyberspace affairs authorities

Critical Information Infrastructure Operators (CIIO)[50] and personal information processors processing personal information shall store personal information collected and generated within the borders of the People's Republic of China if they are reaching quantities provided by the national cyberspace affairs authorities (see Art. 40 PIPL).

Foreign organisations or individuals which are engaged in personal information processing activities and infringe on the personal information of Chinese citizens, or endanger the national security or public interests of China may be restricted. The national cyberspace affairs authorities may add them on a list, make an announcement and take measures such as restricting or prohibiting the provision of personal information (see Art. 42 PIPL).

Personal information processors outside the borders of China (as specified in Art. 3 paragraph 2) shall establish a **specialised agency or a designated representative**

[49] 国家网信部门, guójiā wǎngxìn bùmén.

[50] 关键信息基础设施运营者, guānjiàn xìnxī jīchǔshèshī yùnyíng zhě.

within the borders of China to be responsible for matters related to the protection of personal information. The name of the relevant entity or the name and the contact details of the representative shall be submitted to the department fulfilling personal information protection responsibilities (see Art. 53 PIPL).

In accordance with the provisions of this law, Art. 66 PIPL stipulates **sanctions** if personal information is processed in violation of this law or personal information is processed without fulfilling personal information protection obligations. The departments fulfilling personal information protection responsibilities shall order corrections, give warnings, confiscate illegal income, order the suspension or termination of service of the specialised agency or designated representative within the borders of China responsible for the illegally processed personal information. Where correction is refused, an additional fine of up to 1,000,000 RMB is additionally to be imposed. The directly responsible person and other directly responsible personnel are to be fined between 10,000 and 100,000 RMB.

If the circumstances of the illegal acts mentioned in the preceding paragraph are serious, the provincial or higher-level departments fulfilling personal information protection responsibilities shall order corrections, confiscate illegal income, and impose an additional fine of up to 50,000,000 RMB or up to 5% of the annual revenue.

They may also order the suspension of relevant business activities or the cessation of the business for rectification and inform the responsible department to revoke the relevant business permission or license. The directly responsible person and other directly responsible personnel are to be fined between 100,000 and 1,000,000 RMB and it may also be decided to prohibit them from holding positions of director, supervisor, high-level manager or personal information protection officer for a certain time period.

If there are illegal activities as provided in this law, they shall be recorded in the credit files according to relevant laws and administrative regulations and make known to the public (see Art. 67 PIPL).

The PIPL could affect European R&I entities working on joint research projects with Chinese partners particularly when processing of personal information of natural persons

In summary, the PIPL sets out general principles and places high demands on data processors. Foreign data processors must comply with plenty of regulatory requirements such as the need to assign local representatives and reporting obligations to supervisory agencies in China. It is perfectly legitimate to say that the PIPL "put an end to the Wild West era for China's Big Tech companies, in which they have largely had a free hand in how they collect and use consumer data."[51]

Due to its comparability to the European Union GDPR and its high standard of data protection, data processors can be highly optimistic to meet the requirements. Nevertheless, an individual and detailed examination of the requirements will be absolutely necessary.

8. Conclusion

The collection, processing and use of data within a research and innovation cooperation with Chinese partners not only requires a compliance check pursuant to the European Union GDPR but also a compliance check with Chinese data laws and regulations. It is absolutely necessary to examine if relevant Chinese regulatory requirements have to be

[51] Qu, SCMP, August 20, 2021.

fulfilled. Even in the case where the cooperation partners agree on a European jurisdiction Chinese data laws can still apply.

It is imperative to implement a tailored technical system on data and digital security to manage regulatory risks. R&I partners need to start reviewing and updating data collection and management systems to meet the new compliance obligations.

Before the start of a R&I cooperation project with Chinese partners it is recommended to background check the relevant partner, check of current export control lists, apply timely for required documents, proactively seek advice from relevant authorities when unsure and clarify any other export control issues. Furthermore, it needs to be clarified in advance if the project is funded by the Chinese government to find out whether or not the SDM is applicable. Moreover, a classification of data must be carried out during the whole project. It has to be clarified, whether the data a "personal data", "national core data", "important data" or "general data". The appropriate requirements for data storage, reporting duties, etc. must be respected. In addition, any planned publication must be prepared thoroughly in advance.

A proper compliance with the Chinese measures is also needed to ensure that the researcher and his or her counterparts remain safe while conducting research. In that regard, the possibility of a personal liability might lead to a deterrent effect.

In each individual case, however, a detailed examination of the laws and regulations is absolutely necessary.

It is to be expected that Chinese data-related legislative activities will accelerate in the next years and that the legal and regulatory framework on data protection will be further enhanced and improved.[52] Finally, with the help of these laws and regulations and in the light of the Chinese Communist Party's influence on the application and interpretation of these laws, the Chinese Communist Party is able to shape the future of data flows according to their respective political, economic and social goals. It also remains to be seen how the Chinese Communist Party could use the new data protection rules to regulate the power and competitiveness of the domestic cyberspace sector.

[52] Chen/Han/Kipker, p. 57.