BEAUFTRAGT VOM

Bundesministerium
für Bildung
und Forschung

TaylorWessing

FuE-relevante Datengesetze der VR China

Leitfaden

15. November 2022

Inhaltsverzeichnis

I. Einführung zum Leitfaden

Der hier vorliegende Leitfaden folgt dem Grundsatz, dass wissenschaftliche Zusammenarbeit und Austausch mit chinesischen Forschungsinstituten, Hochschulen, Forschern und Unternehmen grundsätzlich wünschenswert und von hohem Interesse für die deutsche Wissenschaftslandschaft ist. Die Herausforderungen mit Blick auf mögliche Hürden und Zutrittsschranken für eine deutsch-chinesische Forschungskooperation sind in jüngster Zeit stärker thematisiert worden, insbesondere für die Forschung vor Ort in China und die grenzüberschreitende Übermittlung von Forschungsdaten und gewonnenem Know-how aus der Kooperation.

Der Leitfaden weist auf regelungsbedürftige Sachverhalte hin, um Forschung in und mit China auch durch Wahrung der Interessen der Hochschulrektorenkonferenz und ihrer deutschen Forschenden zu ermöglichen. Er ergänzt bestehende Standards wie die Leitfragen zur Hochschulkooperation mit der VR China vom 9. September 2020 und will eine Hilfestellung bieten zur Identifikation potentiell für grenzüberschreitende Forschungsprojekte problematischer neuer Anforderungen im chinesischen Cyberschutz- und Datenschutzrecht mit Blick auf drei zentrale neue Normen, das Data Security Law, in Kraft seit dem 1. September 2021, das Personal Information Protection Law, in Kraft seit dem 1. November 2021 sowie die vom chinesischen Staatsrat erlassenen Measures for the Management of Scientific Data, in Kraft seit dem 17. März 2018.

II. Data Security Law („DSL“)

1. Einführung

Das DSL bildet den grundsätzlichen Rahmen für Datenverarbeitungstätigkeiten, welche innerhalb des Gebiets der VR China durchgeführt werden, einschließlich den damit verbundenen Sicherheitsanforderungen. Soweit Forschungstätigkeiten mit Datenerhebung oder –verarbeitung durch Partner oder selbst vor Ort in China durchgeführt werden, findet diese Norm Anwendung.

Das Gesetz regelt u.a. in Art. 2(2), dass auch Datenverarbeitungsaktivitäten, welche außerhalb des Territoriums der VR China durchgeführt werden, Verantwortung und ggf. Haftung nach diesem Gesetz auslösen, soweit diese Aktivitäten die nationale Sicherheit, die öffentlichen Interessen oder die legitimen Rechte und Interessen von Bürgern oder Organisationen der Volksrepublik China schädigen.

Als Daten werden hierbei gem. Art. 3(1) jede Informationsspeicherung in elektronischer oder anderer Form erfasst, also auch „Papierdaten“. Es findet eine Verhaltensanknüpfung in Verbindung mit einer

datenspezifischen Anknüpfung statt: Datenverarbeitungstätigkeiten, die unter das Gesetz fallen, werden mit gewissen Mindestanforderungen versehen, die bei gewissen Arten von Daten („wichtige Daten“, „Kerndaten des Staates“) zu noch erhöhten Anforderungen führen können.

2. Wichtige Elemente des Gesetzes

a) Anforderungen einer umfassenden Klassifizierung aller Daten: Alle Datenverarbeitungstätigkeiten und alle Informationsnetzwerke im Internet müssen eine Risikoanalyse und Sicherheitsbewertung des eigenen Datensystems nach chinesischen Standards vornehmen und alle Daten klassifizieren, Art. 21 DSL. Zum Verfahren wurden eigene Richtlinien erlassen. Inhaber sog. „wichtiger“ Daten müssen nach dem DSL bei Nutzung des Internets eine regelmäßige Risikoanalyse („risk assessment“) vornehmen und diese den staatlichen Stellen vorlegen.

b) „Wichtige Daten“: Liegen wichtige Daten für das spezifische Projekt nach allgemeinen Kriterien des Cyber Security Law (CSL) oder katalogbasierten Definitionen einzelner Ministerien oder der Cyberspace Administration of China CAC vor – auch hierzu gibt es Entwürfe für die Einordnung und Bestimmung des Vorliegens „wichtiger Daten“ - kann der Export beschränkt, unter Genehmigungsvorbehalt bzw. Auflagen gestellt oder auch untersagt werden. Dieses Erfordernis ist – anders als im CSL – nicht auf Betreiber kritischer Informationsinfrastrukturen beschränkt. Weiter müssen in diesem Fall eindeutig verantwortliches Personal und Management ernannt werden und nachweisbare, strengere Sicherungsmaßnahmen für diese Daten vorgenommen und protokolliert werden. Empfänger von wichtigen Daten im Ausland müssen vertragliche Verpflichtungen zu deren Schutz eingehen, die von den Behörden vorgegeben werden können.

c) Exportkontrolle für Daten: Wichtige Daten dürfen nicht ohne vorherige Risikoeinschätzung sowie Prüfung von Sicherheitsrisiken durch die Behörden ins Ausland exportiert werden. Es gibt eine nach Industriesektoren unterschiedliche Katalog- Auswahl an vor einem Export zu kontrollierenden Daten. „Nationale Kerndaten“ gem. Art. 21 DSL unterliegen noch strengeren Überprüfungskriterien und Sicherheitsanforderungen. Schließlich können in Zukunft Daten auch unter Beschränkungen nach dem Export Control Law fallen.

d) Gesetzlicher Bewertungsmaßstab des Handelns: Jede Datenverarbeitungsaktivität sowie die Erforschung und Entwicklung neuer Datentechnologien muss „dem Fortschritt der wirtschaftlichen und sozialen Entwicklung dienen, das Wohlergehen der Menschen fördern und der gesellschaftlichen Moral und Ethik entsprechen“, Art. 28 DSL.

e) Haftungsrisiken für Organisation und benannte Verantwortliche, Art. 45 ff. DSL: (Persönliche) Haftung u.a. bei ungenehmigten Export von Daten bis zu 10 Millionen CNY, für Individuen bis zu 1 Million CNY, strafrechtliche Risiken bei „nationalen Kerndaten“.

3. Orientierungsfragen und Hinweise

- Datenklassifizierung: Wurde ein Datamapping und eine Untersuchung der Datenströme sowie der beteiligten Datenverarbeiter für die geplante Art und den Umfang der Daten im konkreten Forschungsprojekt (mindestens durch den chinesischen Partner) analysiert und protokolliert, vgl. Art. 21 DSL in Verbindung mit nationalen Standards? Datenverarbeitungsaktivitäten im Internet führen zur zwingenden Anwendung des chinesischen Klassifizierungssystems und entsprechender Sicherheitsmaßnahmen, Art. 27 DSL.
- Export: Sind „nationale Kerndaten“, „kontrollierte Daten“ (Daten, welche von der Exportkontrolle betroffen sind und unter Kataloge nach dem neuen Export Control Law fallen, Art. 25 DSL) mit möglichem Einfluss auf öffentliche Interessen Teil der Forschungskooperation? Soweit dies möglich und Datenexport notwendig ist, muss die Machbarkeit der Kooperation hinterfragt werden.
- „Wichtige Daten“: Das DSL enthält einige allgemeine Bestimmungen, die für den Umgang mit "wichtigen Daten" gelten. Artikel 27 verlangt von den Verarbeitern wichtiger Daten, einen Datenschutzbeauftragten und eine Datenschutzabteilung zu benennen, die für die Erfüllung der Datenschutzverpflichtungen gemäß der DSL verantwortlich sind. Artikel 30 DSL sieht vor, dass die Verarbeiter wichtiger Daten regelmäßige Risikobewertungen ihrer Datenverarbeitungstätigkeiten durchführen und ihrer Aufsichtsbehörde Risikobewertungsberichte vorlegen müssen. In den Risikobewertungsberichten müssen die Arten und Mengen wichtiger Daten, die Art der Verarbeitung wichtiger Daten, die Datensicherheitsrisiken und die Schutzmaßnahmen, um auf die festgestellten Risiken reagieren zu können, angegeben werden. Aus einer Verletzung dieser Anforderungen können Haftungsrisiken nach Art. 45, 46, 48 DSL und anderen Gesetzen entstehen, einschließlich für verantwortliche Führungskräfte und „andere direkt verantwortliche Personen“.
- Vertragliche Regelung: Gibt es für einen Datenexport aus China heraus entsprechende ausdrückliche vertragliche Vereinbarungen zur Verarbeitung und dem Schutz dieser Daten? Können diese Vereinbarungen chinesischen Behörden vorgelegt werden?
- Streitregelung und Art. 36 DSL: Diese Vorschrift kann dazu führen, dass im Streitfall vor Gericht eine Herausgabe von in China gespeicherten Daten (welche z.B. Streitgegenstand des Verfahrens sein können) nicht herausgegeben werden dürfen. Entsprechend müssen Streitregelungsmechanismen in Kooperationsverträgen hierauf angepasste vertragliche Regelungen enthalten.

III. Personal Information Protection Law („PIPL"):

1. Einführung

Das Gesetz knüpft an die Tätigkeit der Verarbeitung personenbezogener Informationen (anstelle einer Anknüpfung nur an „personenbezogenen Daten" per se) natürlicher Personen durch Organisationen und Einzelpersonen innerhalb des Gebiets der Volksrepublik China an.

Während grundsätzlich das PIPL nur Tätigkeiten innerhalb Chinas erfasst, schließt Art. 3 PIPL Datenverarbeitungstätigkeiten in den Schutzbereich des Gesetzes mit ein, welche zwar außerhalb des Gebiets der VR China vorgenommen werden, aber Individuen betreffen und (1) entweder zum Zweck der Bereitstellung von Produkten oder Dienstleistungen für natürliche Personen im Hoheitsgebiet der VR China vorgenommen werden, (2) um das Verhalten natürlicher Personen im Territorium der VR China zu analysieren und zu bewerten, oder (3) als offener Tatbestand für spätere Gesetzgebung bei anderen durch Gesetze und Verwaltungsvorschriften festgelegten Umständen.

Der Begriff der personenbezogenen Informationen und ihre Verarbeitung ist in Art. 4 offen definiert als verschiedene Arten von elektronischen oder anderweitig aufgezeichneten Informationen, die sich auf identifizierte oder identifizierbare natürliche Personen beziehen, mit Ausnahme von anonymisierten Informationen. Die Verarbeitung personenbezogener Informationen umfasst das Sammeln, Speichern, Verwenden, Veredeln, Übermitteln, Bereitstellen oder die öffentliche Bekanntgabe von personenbezogenen Daten.

Als Datenverarbeiter definiert Art. 72 PIPL Organisationen und Einzelpersonen, die unabhängig die Zwecke und Mittel für die Verarbeitung personenbezogener Daten und andere Angelegenheiten der Verarbeitung personenbezogener Daten bestimmen. Eine genaue Unterscheidung zwischen sog. „Verantwortlichen" und „Auftragsdatenverarbeitern" wie in der DSGVO sieht das PIPL nicht vor. Damit bestehen umfangreiche Verpflichtungen nach dem PIPL grundsätzlich auch für Personen oder Organisationen bzw. Gesellschaften, die im europäischen oder deutschen Recht nur als Auftragsverarbeiter anzusehen sind.

Grundsätzlich gilt: Die Einhaltung der DSGVO ersetzt nicht die Befolgung der Anforderungen des PIPL.

2. Wichtige Elemente des Gesetzes

a) Handlungsbeschränkungen: Verbot von Datenverarbeitung, welche gegen chinesische Gesetze und Verordnungen verstößt bzw. Datenverarbeitungsaktivitäten, welche die nationale Sicherheit oder öffentliche Interessen gefährden: Weiter Auffangtatbestand mit Folge einer möglichen Haftung, Art. 10 PIPL, vgl. Art. 42 PIPL u.a. mit der Möglichkeit einer Beschränkung oder Verbots als Empfänger personenbezogener Daten auch im Falle der Verletzung von Rechte und Interessen chinesischer Staatsbürger.

b) Zustimmung des Datensubjekts bzw. Befreiung vom Zustimmungserfordernis: Das PIPL enthält teils weitreichende Anforderungen an das Vorliegen einer – oft ausdrücklichen – zweckgebundenen Zustimmung, vergleichbar mit der DSGVO. Öffentlich verfügbare personenbezogene Daten können gem. Art. 13 PIPL bei Vorliegen gewisser Voraussetzungen ohne Zustimmung verwendet werden, teils auch bei schon öffentlich verfügbaren Daten, allerdings nur „in einem angemessenen Umfang gemäß den Anforderungen des PIPL“. Dies bedeutet, dass von der Cyberspace Administration of China CAC festgelegte Umfänge an Datenmengen nicht zustimmungsfrei sein werden und erfordert ein Monitoring der Gesetzeslage und Praxis.

c) Sensible Daten und Zustimmung (Art. 29 PIPL): Diese erfordern laut Gesetz und entsprechenden Einzelverordnungen je nach Bereich eine „separate“ oder „ausdrückliche“ Zustimmung, müssen mit umfassender Aufklärung über u.a. Zweck, Methode, Art von Daten und Risiken der Datenverarbeitung (Art. 30 PIPL) erteilt werden und unterliegen insbesondere beim Datenexport teilweise besonderen Anforderungen (z.B. Daten Minderjähriger unter 14 Jahren, Zustimmungserfordernis der Eltern, Art. 31 PIPL).

d) Weitergabe von Daten (Auftragsdatenverarbeitung): Diese erfordert ebenfalls „ausdrückliche Zustimmung“, die Weitergabe ist begrenzt auf den angegebenen Datenverarbeitungszweck, Art. 23 PIPL.

e) Gemeinsame Datenverarbeitung: Diese führt zu einer gesamtschuldnerischen Haftung auch für das Verhalten des anderen Datenverarbeiters, Art. 20 PIPL. Es besteht weiter eine Beweislastumkehr zu Lasten des Datenverarbeiters, Art. 69 PIPL.

f) Export und Sicherheitsüberprüfung: Export aus China von personenbezogenen Daten erfordert neben dem Vorliegen einer Rechtfertigungsgrundlage nach Art. 13 PIPL entweder (1) eine vorherige Sicherheitsüberprüfung nach CAC Standards gem. Art. 40 PIPL, (2) eine Zertifizierung zum Datenschutz nach Vorschriften der CAC, oder (3) eine Grundlage eines Standardvertrags, der durch die CAC genehmigt wurde, in welchem vereinbart und sichergestellt sein muss, dass die Datenverarbeitung im Ausland den chinesischen Standards nach dem PIPL entspricht, Art. 38 PIPL. Ein erster Entwurf von Standardvertragsklauseln liegt seit Juni 2022 vor. Danach ist dieser Rechtfertigungsgrund

nicht anwendbar auf Betreiber kritischer Infrastrukturen, Datenverarbeitungen von mehr als 1 Million Datensubjekten oder Export von 100.000 personenbezogenen bzw. 10.000 sensiblen personenbezogenen Datensubjekten seit Januar des der Datenverarbeitung vorangegangen Jahres. Daneben erfordert der Export personenbezogener Informationen an einen Empfänger außerhalb der VR China den organisatorischen oder persönlichen Namen und Kontaktinformationen des ausländischen Empfängers zur Ausübung von Rechten nach dem PIPL, Art. 39 PIPL. Vor dem Export ist eine Datenfolgenschutzabschätzung nach Art. 55 PIPL erforderlich.

g) Pflicht zur lokalen Datenspeicherung: Sowohl Betreiber kritischer Infrastrukturen als auch allgemeine Datenverarbeiter, dieeine von der Datenschutzbehörde festgelegte Menge überschreiten (s.o. 6.), müssen gesammelte oder selbst in China generierte personenbezogene Daten in China speichern. Ihr Export erfordert „tatsächliche Notwendigkeit“ und das Durchlaufen einer Sicherheitsüberprüfung der CAC, sofern diese nicht nach anderen Vorschriften entbehrlich ist, Art. 40 PIPL.

h) Credit Ranking im neuen chinesischen Sozialkreditsystem: Es besteht das Risiko eines Blacklistings im Falle der Verletzung der Rechte und Interessen chinesischer Bürger oder Gefährdung des öffentlichen Interesses oder der nationalen Sicherheit, Art. 42, 66 PIPL.

i) Datenschutzbeauftragter: Es besteht eine Pflicht bei Erreichen von durch CAC festgelegten Schwellenwerten zur Ernennung und Mitteilung eines Data Protection Officer nach Art. 52 PIPL an die chinesischen Behörden, sowie eine umfangreiche Risikoanalyse mit Gegenmaßnahmen im Falle eines Datenvorfalls. Art. 54 PIPL schreibt ein „regelmäßiges Audit“ der Datenverarbeitung vor.

j) Inländischer Vertreter: Datenverarbeitung außerhalb Chinas, welche die Voraussetzungen des Art. 3 Abs. 2 PIPL erfüllt, führt zu einer Pflicht zur Benennung eines inländischen Vertreters („Agent or representative“) für ausländische Datenverarbeiter und Benennung der Nominierung gegenüber der CAC, Art. 53 PIPL. Für diese Person entstehen persönliche Haftungsrisiken nach Art. 66 PIPL.

3. Orientierungsfragen und Hinweise

- Sicherstellung der Zustimmung bzw. Befreiung: Bei Zustimmungserfordernissen (d.h. kein Fall des Art. 13 PIPL mit Entfallen des Zustimmungserfordernisses) Erstellen des Nachweises, dass Identität und Kontaktinformationen des Datenverarbeiters, Zweck, Umfang, Empfänger und Methode der Datenverarbeitung, Art von personenbezogenen Daten und Aufbewahrungsfrist, Methoden und Verfahren zur Wahrnehmung von Rechten von Einzelpersonen auf Chinesisch klar und verständlich, leicht abrufbar, speicherbar und öffentlich verfügbar sind und dass Zustimmung erteilt wurde.

- Sensible Daten: Bei Einholen einer Zustimmung muss der die Daten erhebende Partner bzw. der deutsche Forscher die Anforderungen der Art. 14 (spezifische Zustimmung, wiederholtes Einholen bei Zweckänderung, Datenverarbeitungsmethode oder Art der personenbezogenen Daten), Art. 17 PIPL (klare verständliche Sprache, Kontaktinformationen usw.) sowie weitergehende Anforderungen für sensible Daten Art. 28 ff. PIPL einhalten (weitergehende ausdrückliche Zweckbegrenzung, Notwendigkeit der Datenverarbeitung, strikte Sicherheitsmaßnahmen), anderenfalls kann gem. Art. 20 eine gemeinsame Haftung begründet werden. Weiter findet gem. Art. 69 PIPL bei zivilen Ansprüchen von Datensubjekten eine Beweislastumkehr statt.
- Weitergabe von Daten: Bei Weitergabe von personenbezogenen Daten an andere Personen muss einerseits eine ausdrückliche Zustimmung des Datensubjekts vorliegen, Art. 25 PIPL, und der Empfänger muss alle notwendigen Maßnahmen zum Schutz der personenbezogenen Daten ergreifen, Art. 59 PIPL. Andererseits muss bei Auftragsverarbeitung die Identität, der Kontakt, Art der Daten, Verarbeitungsmethode und Zweck der Verarbeitung dem Datensubjekt mitgeteilt und eine ausdrückliche Zustimmung eingeholt werden, Art. 21 PIPL. Daher sollte bei Forschungsprojekten mit hoher Wahrscheinlichkeit der Anforderung einer „Verkehrsfähigkeit“ von personenbezogenen Daten vorab Mechanismen für ein Zustimmungseinholen mit den richtigen Angaben und im vorgeschriebenen Umfang sichergestellt werden (ggf. per vertraglicher Verpflichtung des chinesischen Partners, hierfür Sorge zu tragen). Für Forschungsaktivitäten, welche die Weitergabe von personenbezogenen Daten erfordern, sollte dieses Erfordernis von Anfang an in die Aufklärung und ausdrückliche Zustimmung des Datensubjekts mit aufgenommen werden.
- Haftungsvereinbarung und -freistellung: Vereinbarung bei gemeinsamen Datenverarbeitungstätigkeiten nach Art. 20 PIPL, welche (1) die interne Haftung klarstellt, (2) ein Recht gibt, bei Anfragen von Einzelpersonen wegen ihrer Datenschutzrechte Unterstützung und Auskunft durch den Vertragspartner zu erhalten und ggf. die Ausübung von Widerrufsrechten des Datensubjekts umzusetzen, sowie (3) Haftungsfreistellung im Innenverhältnis bei Fehlverhalten des Vertragspartners.
- Verarbeitung durch staatliche Stellen: Soweit „staatliche Stellen“ die personenbezogenen Daten in China verarbeiten, muss vor jeglichem Export eine Genehmigung und Risikobewertung vorab durchgeführt werden, Art. 36 PIPL. Hierbei wird der Begriff „staatliche Stellen“ gem. Art. 37 PIPL erweitert auf jegliche Organisation, welche eine „Managementfunktion für öffentliche Angelegenheiten nach Gesetz oder Verordnung unternimmt“. Klärung mit dem Forschungspartner vorab, ob Art. 36 PIPL Anwendung findet.
- Export: Bei jeglichem Datenexport von personenbezogenen Daten ist entweder (1) eine Sicherheitsüberprüfung nach Art. 40 PIPL vorzunehmen, oder (2) eine Zertifizierung durch

eine von der CAC genehmigte Zertifizierungsstelle, oder (3) ein von der CAC genehmigter Standardvertrag mit Verweis auf Pflichten nach dem PIPL abzuschließen. Für Betreiber kritischer Informationsinfrastrukturen bzw. bei großen Datenmengen ist eine Sicherheitsüberprüfung zwingend, Art. 40 PIPL. Standardverträge nach DSGVO sind weiter nicht ausreichend, um für den Datenexport Compliance mit den chinesischen Gesetzen herzustellen. Es ist eine separate, von CAC genehmigte Version zu verwenden, um Zustimmung zum Export zu fingieren. Die Parteien treffen Absprachen, wie im Falle eines Verbots oder einer Einschränkung des Exports das Projekt weiterzuführen oder ggf. zu beenden ist.

- Sicherheitsüberprüfung: Für jedes Projekt müssen eine Risikoeinschätzung der Sensitivität der personenbezogenen Daten und möglichen Auswirkungen bei einem Datenvorfall sowie eigene Verfahren und Sicherheitsvorkehrungen nach Art. 51 PIPL möglich, umsetzbar und darstellbar sein. Prüfung, ob nach Art. 52 PIPL wegen hoher Volumina ein lokaler Datenschutzbeauftragter benannt werden muss und den Behörden mitgeteilt wird. Damit im Zusammenhang stehende Haftungs- und Versicherungsfragen (Art. 61 ff. PIPL, insbesondere Art. 65 PIPL) müssen adressiert werden.
- Inländischer Vertreter: Art. 53 PIPL erfordert für ausländische Datenverarbeiter, einen designierten Vertreter bzw. Repräsentanten im chinesischen Inland als Verantwortlichen zu benennen und den Behörden bekannt geben zu müssen. Der chinesische Forschungspartner muss hierzu ggf. verpflichtet werden, um die Haftung eigener Repräsentanten/Forscher innerhalb Chinas zu begrenzen.

IV. Measures for the Administration of Scientific Data („SDM“)

1. Einführung

Voraussetzung für die Anwendbarkeit der SDM ist die Einordnung einer Forschungstätigkeit mit “wissenschaftlichen Daten” wie in Art. 2 SDM definiert. Die gesetzliche Definition deckt alle Arten von Forschung und Entwicklung in China ab, einschließlich Daten, die aus der Grundlagenforschung, der Anwendungsforschung, der Pilotentwicklung und anderen Bereichen wie Naturwissenschaft und Ingenieurtechnik stammen, sowie Originaldaten und abgeleitete Daten, die durch Beobachtung und Überwachung, Umfrage und Untersuchung sowie Inspektion und Erkennung gewonnen und für die wissenschaftliche Forschung verwendet werden.

Art. 3 SDM bestimmt den inhaltlichen Anwendungsbereich der SDM: Sie gelten für alle Aktivitäten (Sammeln, Gewinnung, Verarbeitung, Anordnung, Veröffentlichung und Teilen sowie Management und Gebrauch) in Bezug auf wissenschaftliche Daten, welche mit „Haushaltsmitteln der

Regierung“ unterstützt werden. Der Anwendungsbereich wird nach Art. 3(2) SDM erweitert auf Aktivitäten (nach der offenen Formulierung auch auf solche außerhalb Chinas), welche sich auf solche Aktivitäten mit Bezug auf Forschungsdaten innerhalb der VR China „beziehen“.

2. Wichtige Elemente der Verordnung

a) Zwingende Übermittlung an chinesische Datenzentren: Zwingende Einreichung wissenschaftlicher Daten bei chinesischen Datenzentren, Art. 13, 15 SDM.
b) Zwingende Standards: Aufbereitung der Datensätze nach chinesischen Standards erforderlich, Art. 11 SDM.
c) Veröffentlichungen: Zwingende Einreichung von mit Haushaltsmitteln geförderten wissenschaftlichen Daten sowie mit „social funds“ geförderten Daten mit Relevanz für nationale Sicherheit, Staatsgeheimnisse oder öffentliche Interessen für nationalen oder internationale Veröffentlichungen in Wissenschaftsjournalen vor ihrer Veröffentlichung, Art. 14 SDM.
d) Open Access Grundsatz: Grundsatz der Veröffentlichung und des Zugänglichmachens von eingereichten wissenschaftlichen Daten auf den Plattformen der nationalen Data Centers, Art. 19 SDM. Handelsgeheimnisse sollen geschützt werden, können aber im Falle absoluter Notwendigkeit nach einer Einzelfallprüfung eingeschränkt öffentlich zugänglich gemacht werden, Art. 25 SDM.
e) Zwangslizenz: Mögliche Zwangslizenz (grundsätzlich kostenlos, anderenfalls nach dem Grundsatz der Gemeinnützigkeit festgelegt) auf wissenschaftliche Daten, welche zur Entscheidungsfindung der Regierung, die öffentliche Sicherheit, den Aufbau der Landesverteidigung, den Umweltschutz, die Katastrophenvorbeugung und Schadensbegrenzung sowie für die wissenschaftliche Forschung ohne Erwerbszweck benötigt werden, Art. 24 SDM.

3. Orientierungsfragen und Hinweise

- Anwendung der SDM: Klarstellung vor Unterzeichnung eines Projekts, ob das Projekt direkt oder – unter Feststellung der Art und Weise und des Umfangs – indirekt durch Haushaltsmittel der chinesischen Regierung unterstützt wird. Falls dies bestätigt ist, muss verifiziert werden, ob und inwiefern die Übermittlung und Veröffentlichung der wissenschaftlichen Daten in Datenzentren der chinesischen Regierung unproblematisch ist. Bei dieser Einschätzung sollen auch fortlaufend später im Projekt generierte wissenschaftliche Daten berücksichtigt werden, da diese gem. Art. 13 SDM ebenfalls (nachträglich) eingereicht werden müssen.

- Erweiterter Anwendungsbereich: Art. 15 SDM sieht weiter eine zwingende Einreichung vor für wissenschaftlichen Daten, die mit Unterstützung von „Sozialfonds“ gebildet wurden und Staatsgeheimnisse, die Staatssicherheit oder die gesellschaftlichen öffentlichen Interessen berühren. Eine Definition von „social funds“ findet sich nicht im Gesetz oder der SDM. Klärung vor Beginn eines Projekts, ob diese Vorschrift Anwendung findet und dies den Projektzielen entgegenstehen könnte. Ggf. Ausschluss und Garantie der Finanzierung eines Forschungsprojekts mit „Haushaltsmitteln der VR China“ sowie Anzeigepflicht des chinesischen Partners, falls er zu einer Übermittlung an chin. Datenzentren aufgefordert wird.
- Chinesische Standards Datenaufbereitung: Soweit Aktivitäten zu wissenschaftlichen Daten in China mit Haushaltsmitteln unterstützt werden, Prüfung, ob und welche Standardvorgaben der chinesischen Regierung zu Datensätzen „in einfacher, durch die chinesische Regierung nutzbarer Form“ bereitgestellt werden können und sollen, Art. 11 SDM.
- Veröffentlichungen: Bei Veröffentlichungen in oder außerhalb Chinas von wissenschaftlichen Daten, welche mit Unterstützung chinesischer Haushaltmittel gewonnen wurden, sind diese vor Veröffentlichung bei der Einrichtung, zu welcher der chinesische Forschungspartner gehört, zur Verwaltung einzureichen.
    - Soweit diese Daten vertraulich behandelt werden und nicht veröffentlicht werden sollen, ist dies auf der Veröffentlichung zu vermerken, damit gemäß Art. 25 SDM eine Veröffentlichung unterbleibt. Dieser Schutz ist allerdings nicht absolut, denn soweit die Veröffentlichung „absolut notwendig“ ist, findet eine Prüfung und ggf. eingeschränkte Veröffentlichung statt. Im Grundsatz kann damit die chinesische Verwaltung dennoch gem. Art. 19 SDM eine Veröffentlichung und Teilen mit Regierungsstellen durchsetzen.
    - Soweit patentrechtlich relevante Daten enthalten sind, kann die Übermittlung zur neuheitsschädlichen Veröffentlichung vor Anmeldung führen. Es müssen geeignete Absprachen mit dem chinesischen Forschungspartner getroffen werden, welcher die Daten übermittelt, damit dies ausgeschlossen werden kann.
    - Prüfung, ob durch diese Vorabübermittlung Verlagsverträge verletzt werden könnten, insbesondere soweit auch Übersetzungen ins Chinesische in die Rechte des Verlags fallen oder eine Nichtübergabe an Dritte bzw. keine Veröffentlichung durch dritte Stellen vertraglich zugesagt wurde.
    - Ethische Bedenken wegen einer möglichen Nutzung der wissenschaftlichen Daten durch das chinesische Militärmüssen berücksichtigt und für eine grundsätzliche Machbarkeit des konkreten Forschungsprojekts geprüft werden: Art. 19 SDM spricht explizit vom Ziel eines Austauschs zwischen der People’s Liberation Army PLA (Militär) und wissenschaftlichen Daten in den nationalen Datenplattformen, auch welche die wissenschaftlichen Daten eingestellt werden.

- Open Access und Proprietäre Forschung: Soweit die wissenschaftlichen Daten proprietär bleiben sollen bzw. einer Geheimhaltung unterliegen, ist eine Durchführung der Forschung unter den SDM problematisch, da die Art. 20 bis 22 SDM zu einer Behandlung als open access führen, auch wenn Art. 23 SDM die Einhaltung von IP-Rechten vorschreibt.
- Zwangslizenz: Prüfung vorab, ob ein Risiko einer erzwungenen Nutzungserlaubnis für öffentliche Stellen und die gemeinnützige Forschung in China sowie eine mögliche Zwangslizenz nicht hingenommen werden kann, Art. 24 SDM.

15. November 2022

Dr. Thomas Pattloch