DAAD KIWi

Deutscher Akademischer Austauschdienst
German Academic Exchange Service

KIWI KOMPASS

Datenschutz in China

Implikationen chinesischer Datenschutzregelungen in akademischen Kooperationen

www.daad.de/kiwi

Regularien
Definitionen
Praxis

Inhalt

1

Einleitung

Der transnationale Datenverkehr spielt in allen internationalen Hochschulpartnerschaften eine wichtige Rolle. Dies gilt insbesondere für Kooperationen mit chinesischen Partnern. Mit der zunehmenden Reglementierung des nationalen und grenzüberschreitenden Datenverkehrs durch die Regierung der Volksrepublik China stehen Hochschulkooperationen und Forschungsprojekte einer doppelten Herausforderung gegenüber: Sie sollen zugleich Kenntnisse über die bestehende Gesetzeslage zum Datenschutz in Europa als auch in China besitzen und auf dieser Grundlage über die Optionen einer Kooperation im Rahmen der bestehenden Reglementierungen entscheiden. Bei der Ausgestaltung von Partnerschaften zwischen Hochschulen in Deutschland und China müssen also Entscheidungsträgerinnen und -träger in Forschung, Lehre und Verwaltung die Vorteile einer Kooperation mit China aus einem institutionellen und wissenschaftlichen Interesse gegenüber den möglichen Risiken abwägen.

Um eine Chancen-Risiken-Abwägung zu erleichtern und grundlegende China-Kompetenzen zu vermitteln, bietet der Deutsche Akademische Austauschdienst (DAAD) mit dem Kompetenzzentrum Internationale Wissenschaftskooperationen (KIWi) wichtige Informationen und Hinweise für Mitglieder deutscher Hochschulen in China-Kooperationen. Der vorliegende KIWi Kompass „Datenschutz in China. Implikationen chinesischer Datenschutzregelungen in akademischen Kooperationen“ entstand aufgrund der erhöhten Nachfrage, die das KIWi zu diesem Thema erreichte. Hiermit wird eine Übersicht der zentralen datenschutzrelevanten Gesetze und Vorschriften in China, die seit Januar 2026 für Kooperationsprojekte ausländischer Partner mit China gelten, vorgestellt. **Zudem werden Handlungsoptionen formuliert, die nach einer sorgfältigen Prüfung möglicher Risiken beim Transfer, der Nutzung oder Speicherung von Daten die Weiterführung oder Etablierung von Kooperationsprojekten erleichtern sollen.** Somit weitet das KIWi das Portfolio der Wissensprodukte des DAAD zu China aus. Zu diesen gehören die DAAD-Handreichung „Die akademische Zusammenarbeit mit China realistisch gestalten“, die Länderinformationen zu China und die Bildungssystemanalyse China.

Der KIWi Kompass „Datenschutz in China“ spricht zunächst die **Rechtsabteilungen und Justiziariate** der an Kooperationen beteiligten Hochschulen an. Interessierte Wissenschaftlerinnen und Wissenschaftler sowie Mitglieder von Hochschulverwaltungen finden hier ebenfalls Handlungsempfehlungen. Der Schwerpunkt dieser Handreichung liegt dabei ausdrücklich auf chinesischen Bestimmungen, die hier erstmals für den Kontext der deutsch-chinesischen Hochschulkooperationen kompakt dargestellt werden, und nur in wenigen Fällen auf den parallel geltenden europäischen Vorschriften. Dadurch soll das Bewusstsein für die bestehende Gesetzgebung geschärft und die Handlungssicherheit gestärkt werden. Auf dieser Grundlage können informierte Entscheidungen über die **Möglichkeiten und Grenzen der Forschungszusammenarbeit mit China** getroffen werden, die einen interessenorientierten, risikoreflexiven und kompetenzbasierten Dialog mit den Partnern ermöglichen.

Sollte sich für eine Kooperation mit einer chinesischen Partnerhochschule entschieden werden, legt diese Handreichung eine **Transparenzklausel** vor, die in Kooperationsverträge eingefügt werden kann. Zudem bietet der KIWi Kompass in der Anlage ein Abkürzungsverzeichnis mit Definitionen der wichtigsten Begrifflichkeiten sowie die **Checkliste zu chinesischen Datenschutzregelungen in akademischen Kooperationen** anhand derer Kooperationsvorhaben geprüft und bewertet werden können. Für grundsätzliche Fragen der Risikoabwägung in akademischen Kooperationen werden die **weiteren Publikationen des KIWi, wie die** KIWi Checkliste Wissenssicherheit **und der** KIWi Kompass „Keine roten Linien“ **empfohlen**.

HINWEIS

Dieser Kompass soll nur einen ersten Überblick zum Thema geben. Er erhebt keinen Anspruch auf Vollständigkeit und kann eine rechtliche Beratung und Prüfung im Einzelfall nicht ersetzen. Eine Haftung des DAAD für den Inhalt der Publikation ist – außer bei Vorsatz oder grober Fahrlässigkeit – ausgeschlossen.

2

Zur Bedeutung von chinesischen Datenschutzgesetzen in akademischen Kooperationen

Die Nutzung und der Schutz von Daten nehmen in China einen immer größeren Stellenwert ein. Bereits im Jahr 2020 erklärte der Staatsrat der Volksrepublik China Daten als fünften „Produktionsfaktor". So sollen neben Land, Arbeitskraft, Kapital und Technologie auch Daten als Ressource für die wirtschaftliche Entwicklung des Landes genutzt werden. Gleichzeitig wurde sowohl der Schutz von Daten aus einem nationalen Sicherheitsinteresse als auch der Schutz personenbezogener Daten der Bevölkerung, ähnlich der europäischen Gesetzgebung, reglementiert. Trotz dieses verstärkten Fokus verbleiben insbesondere im Bereich der Reglementierung des transnationalen Datenverkehrs sowie bei der Erstellung und Verarbeitung von Forschungsdaten erhebliche Definitionslücken und Grauzonen.

Eine Herausforderung im Umgang mit den auf chinesischer Seite bestehenden Gesetzen und Richtlinien besteht nicht nur darin, dass diese komplex und dynamisch sind, sie lassen sich auch nicht immer mit europäischen Vorgaben in Einklang bringen. Datenschutz ist somit kein rein national zu lösendes Phänomen, sondern stets Teil des Kooperationsmanagements mit internationalen Partnern. Darüber hinaus besteht auch bei chinesischen Kooperationspartnern zwar weiterhin ein hohes Interesse an Internationalisierung, aber oftmals kein oder nur begrenztes Wissen über die aktuelle Gesetzeslage im Bereich des Datenschutzes und ihre damit verbundenen Verpflichtungen.

In den meisten Fällen liegen die gesetzlichen Verpflichtungen auf Seiten der chinesischen Universitäten, Forschungseinrichtungen sowie Forschenden. Dies gilt auch, wenn die Mitglieder deutscher Hochschulen während eines Forschungsaufenthalts in China mit Daten umgehen.

Die gesetzlichen Sanktionen betreffen daher in erster Linie die chinesischen Einrichtungen und deren Mitglieder. Bislang sind keine Fälle bekannt, in denen ausländische Hochschulpartner aufgrund von Datenschutzverstößen ihrer chinesischen Partnerinstitutionen mit Straf- oder Verwaltungssanktionen belegt wurden. Einen größeren Einfluss für die deutschen Partnereinrichtungen haben die chinesischen gesetzlichen Bestimmungen im Fall einer gemeinsamen chinesisch-ausländischen Einrichtung in China (beispielweise einer deutsch-chinesischen Universität), die die entsprechenden gesetzlichen Verpflichtungen trägt, oder für einzelne deutsche Forschende mit Sitz in China, insbesondere beim Export von Forschungsdaten.

Allerdings können deutsche Einrichtungen indirekt von der Sanktionierung ihrer chinesischen Partner betroffen sein. So kann die zuständige Behörde beispielsweise die Aussetzung oder das Verbot grenzüberschreitender Datenübertragungen anordnen, bis die erforderlichen Korrekturmaßnahmen umgesetzt sind. Zudem besteht im Fall einer vorsätzlichen oder grob fahrlässigen Missachtung der chinesischen Gesetze dennoch ein gewisses verwaltungsrechtliches Risiko für die deutschen Hochschulen bzw. deren Wissenschaftlerinnen und Wissenschaftler. Die Cyberspace Administration of China (CAC) kann der betreffenden Organisation oder Person die Bereitstellung personenbezogener Daten einschränken oder untersagen.

Externe Dienstleister, wie spezialisierte Anwaltskanzleien, können Einrichtungen in Deutschland im Einzelfall unterstützen. Dazu kann die Beauftragung eines „Datenschutz-Gesundheitschecks“ gehören, bei dem es sich um eine begrenzte Due-Diligence-Prüfung zur Ermittlung relevanter Risiken und rechtlicher Verpflichtungen handelt. Jedes Kooperationsprojekt muss individuell und auf der Grundlage der neuesten Gesetze und Vorschriften geprüft werden. Je nach Kooperationsprojekt können zusätzliche Gesetze und Vorschriften zur Anwendung kommen. Für Einrichtungen in Deutschland besteht die Möglichkeit, eine staatlich finanzierte juristische Starthilfe zu beantragen.[1]

1 Das BMFTR-finanzierte Angebot der sog. Juristischen Erstberatung für wissenschaftliche Kooperationen im nicht-wirtschaftlichen Bereich mit China wird fortgeführt. Für weitere Informationen kontaktieren Sie das Chinateam des DLR-PT unter chinateam@dlr.de.

3

Relevante Datenschutzgesetze und -regelungen in China

Die Datenschutz- und Cybersicherheitsgesetze der Volksrepublik China (VR China) werden in erster Linie durch drei wichtige Vorschriften geregelt: das Gesetz zum Schutz personenbezogener Informationen (PIPL), das Cybersicherheitsgesetz (CSL) und das Datensicherheitsgesetz (DSL). Diese Gesetze sehen strenge Kontrollen der Datenverarbeitung, -übertragung und -speicherung vor und legen den Schwerpunkt auf die Lokalisierung von Daten, die nationale Sicherheit und den Schutz der Privatsphäre der Nutzerinnen und Nutzer. Das PIPL **spiegelt verschiedene Aspekte der Datenschutz-Grundverordnung (DSGVO) der EU wider** und verlangt von den Unternehmen, dass sie die Zustimmung zur Datenerfassung einholen und strenge Regeln für den Umgang mit personenbezogenen Informationen befolgen. Darüber hinaus werden grenzüberschreitende Datenübertragungen stark reguliert, um sensible und kritische Daten zu schützen.

Daher sollten sich deutsche Einrichtungen als Empfänger von Daten aus China der chinesischen Gesetzen und Vorschriften bewusst sein. Im Falle einer Forschungskooperation ist der Datenempfänger und Kooperationspartner in der Regel die Einrichtung in Deutschland.

Zur Vereinfachung und Erleichterung eines systematischen Ansatzes können Einrichtungen in Deutschland die bereitgestellte **Checkliste zu chinesischen Datenschutzregelungen in akademischen Kooperationen** verwenden. Um das Bewusstsein zu schärfen und relevante Informationen zu erhalten, kann eine **Klausel** in die entsprechende(n) Vereinbarung(en) aufgenommen werden, die der chinesischen Kooperationseinrichtung verschiedene vertragliche Verpflichtungen auferlegt, siehe **4.1** unten.

3.1 Gesetz zum Schutz personenbezogener Informationen (PIPL) (2021)

Das PIPL ist seit dem 1. November 2021 in Kraft. Die wichtigsten zuständigen Behörden sind die Cyberspace Administration of China (**CAC**) und die Public Security Bureaus (**PSB**).

Für die Verarbeitung personenbezogener Informationen verlangt das PIPL die Einhaltung der folgenden **allgemeinen Grundsätze**: Rechtmäßigkeit, Legitimität, Notwendigkeit und Treu und Glauben,[2] bestimmte und angemessene Zwecke,[3] minimaler Umfang und direkter Bezug zu den Zwecken,[4] Offenheit und Transparenz der Verarbeitungszwecke und -methoden,[5] Genauigkeit und Vollständigkeit,[6] und Ergreifen von Sicherheitsmaßnahmen.[7] Die DSGVO hat ähnliche Grundsätze in Bezug auf die Verarbeitung personenbezogener Informationen, nämlich Rechtmäßigkeit, Fairness und Transparenz, Zweckbindung, Datenminimierung, Genauigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, Rechenschaftspflicht.

Informationspflicht: Ähnlich wie bei der DSGVO, **muss** der Verarbeiter personenbezogener Informationen die Personen vor der Verarbeitung der Daten über Folgendes **informieren**:

(i) die Bezeichnung oder den Namen und die Kontaktperson des Verarbeiters der personenbezogenen Informationen;
(ii) den **Zweck und die Methode der Verarbeitung** personenbezogener Informationen sowie die Art und den Aufbewahrungszeitraum der verarbeiteten personenbezogenen Informationen;
(iii) die **Art und Weise und das Verfahren, wie die oder der Einzelne die gesetzlich** vorgesehenen Rechte **ausüben kann.**[8]

DEFINITION

Personenbezogene Informationen werden im CSL (dem zuerst verabschiedeten Gesetz) als verschiedene Informationen definiert, die in elektronischer oder anderer Form aufgezeichnet und allein oder in Kombination mit anderen Informationen verwendet werden, um die Identität einer natürlichen Person zu erkennen, einschließlich: Namen, Geburtsdatum, ID-Nummer, personenbezogene biometrische Informationen, Adresse und Telefonnummer der natürlichen Person.[9]

DEFINITION

Sensible personenbezogene Informationen werden im PIPL als personenbezogene Informationen definiert, die die persönliche Würde einer natürlichen Person verletzen oder ihre persönliche oder materielle Sicherheit beeinträchtigen können, wenn sie offengelegt oder unrechtmäßig verwendet werden. Dazu gehören Informationen wie biometrische Identifikation, religiöse Überzeugung, spezifische Identität, medizinische Gesundheit, Finanzkonten und Aufenthaltsort und Spuren sowie die personenbezogenen Informationen von Minderjährigen unter 14 Jahren.[10]

2 Artikel 5 PIPL.
3 Artikel 6 PIPL.
4 Artikel 6 PIPL.
5 Artikel 7 PIPL.
6 Artikel 8 PIPL.
7 Artikel 9 PIPL.
8 Artikel 17 PIPL.
9 Artikel 76 CSL.
10 Artikel 28 PIPL.

Betroffene Personen haben in China gesetzliche Rechte: Ähnlich wie bei der DSGVO ist das Recht umfasst, Kenntnis von der Verarbeitung personenbezogener Informationen zu erlangen, Entscheidungen hierüber zu treffen, die Verarbeitung ihrer personenbezogenen Informationen durch andere **einzuschränken oder zu verweigern**, ihre personenbezogenen Informationen einzusehen oder zu kopieren, Korrekturen oder Ergänzungen zu verlangen, **die Löschung personenbezogener Informationen zu fordern sowie das Recht**, ihre personenbezogenen Informationen an einen anderen Datenverarbeiter **zu übertragen** (Datenportabilität).[11]

Allgemeine Zustimmungspflicht: Der Verarbeiter personenbezogener Informationen muss in der Regel die (widerrufliche) Einwilligung von Personen einholen, bevor er personenbezogene Informationen verarbeitet, es sei denn, es gilt eine Ausnahme. In Zweifelsfällen **sollte die Einwilligung eingeholt werden**. Die Person muss auch darüber informiert werden, wie die Einwilligung widerrufen werden kann.

Relevante Ausnahmen, für die keine Zustimmung erforderlich ist: Wenn die Datenübermittlung

(i) für den Abschluss oder die Erfüllung eines Vertrags erforderlich ist, bei dem die betroffene Person Vertragspartei ist, zum Beispiel wenn chinesische Studierende einen Vertrag über Studiengebühren mit einer Einrichtung in Deutschland schließen, oder

(ii) für die Implementierung der Personalverwaltung erforderlich ist, wenn zum Beispiel personenbezogene Informationen im Rahmen des Personalmanagements von einer chinesischen Arbeitgeberin oder einem chinesischen Arbeitgeber an eine Einrichtung in Deutschland als Hauptsitz exportiert werden. [12]

Gesonderte Zustimmungspflicht: Der Verarbeiter personenbezogener Informationen muss in den folgenden Fällen eine gesonderte (widerrufliche) Einwilligung von Personen einholen, bevor er personenbezogene Informationen verarbeitet:

(i) wenn ein Auftragsverarbeiter die personenbezogenen Informationen an einen anderen Auftragsverarbeiter weitergibt, wenn zum Beispiel die chinesische Universität personenbezogene Informationen an eine andere Einrichtung zum Zweck der Projektzusammenarbeit übermittelt. Dies kann eine Agentur sein, die bei der Vorbereitung des Austauschsemesters chinesischer Studierender in Deutschland unterstützt;[13]

(ii) wenn ein Auftragsverarbeiter die personenbezogenen Informationen veröffentlicht;[14]

(iii) wenn sensible personenbezogene Informationen verarbeitet werden, zum Beispiel, wenn eine chinesische Universität die Nummer eines Reisepasses/eines Personalausweises, ein ärztliches Gesundheitszeugnis von Lehrenden oder Studierenden verarbeitet; [15]

(iv) wenn die personenbezogenen Informationen an einen Empfänger im Ausland übermittelt werden, zum Beispiel, wenn chinesische Universitäten oder deutsche Forschende in China personenbezogene Informationen an eine Einrichtung in Deutschland übermitteln.[16]

11 Artikel 44 bis 50 PIPL.

12 Weitere gesetzliche Ausnahmen sind: Wenn die Datenübermittlung (iii) für die Erfüllung gesetzlicher Aufgaben oder Pflichten notwendig ist; (iv) für die Reaktion auf einen Notfall im Bereich der öffentlichen Gesundheit oder für den Schutz des Lebens, der Gesundheit und der Sicherheit von Eigentum einer natürlichen Person notwendig ist; (v) wenn bestimmte Handlungen im öffentlichen Interesse durchgeführt werden, wie z. B. Nachrichtenberichterstattung und Überwachung durch öffentliche Meinung, und die Verarbeitung personenbezogener Informationen in einem angemessenen Umfang erfolgt; (vi) wenn die Verarbeitung der von der betroffenen Person offengelegten personenbezogenen Informationen oder anderer personenbezogener Informationen, die rechtmäßig offengelegt wurden, erforderlich ist und sich in einem angemessenen Rahmen bewegt, der durch das PIPL erlaubt ist, und (vii) unter anderen Umständen, die durch Gesetze und Vorschriften vorgeschrieben sind, siehe Artikel 13 PIPL.

13 Artikel 23 PIPL.

14 Artikel 25 PIPL.

15 Artikel 29 PIPL.

16 Artikel 39 PIPL.

Eine **Datenschutz-Folgenabschätzung (PIPIA)** muss in den folgenden Fällen erstellt und mindestens drei Jahre lang archiviert werden:

(i) wenn eine besondere Zustimmung erforderlich ist (siehe oben);
(ii) wenn ein Auftragsverarbeiter die personenbezogenen Informationen an beauftragte Parteien zur Verarbeitung weitergibt;
(iii) wenn personenbezogene Informationen verwendet werden, um eine automatische Entscheidung zu treffen;
(iv) im Falle anderer Verarbeitungen personenbezogener Informationen, die erhebliche Auswirkungen auf die persönlichen Rechte und Interessen haben.[17]

Die DSGVO sieht eine ähnliche Datenschutz-Folgenabschätzung für bestimmte Datenverarbeitungsszenarien vor.

Für die **Übermittlung personenbezogener Informationen ins Ausland** muss der Verarbeiter der personenbezogenen Informationen eine der folgenden Bedingungen erfüllen:

(i) Bestehen einer Sicherheitsbewertung durch die CAC; oder
(ii) Zertifizierung durch eine spezialisierte Agentur; oder
(iii) Abschluss eines von der CAC formulierten Standardvertrags mit dem Empfänger im Ausland, der bei der CAC eingereicht werden muss.[18] Der Standardvertrag ist vergleichbar mit dem SCC unter der DSGVO.

Das PIPL umreißt auch die **allgemeinen Pflichten eines Verarbeiters personenbezogener Informationen**. Dazu gehören die Formulierung interner Managementsysteme und Betriebsverfahren, die Umsetzung einer kategoriebasierten Verwaltung personenbezogener Informationen, die Ergreifung entsprechender technischer Sicherheitsmaßnahmen wie Verschlüsselung und De-Identifizierung, die Festlegung der Befugnisse für den Umgang mit personenbezogenen Informationen und die regelmäßige Durchführung von Sicherheitsschulungen und -trainings für die betreffenden Mitarbeitenden, die Formulierung und Organisation der Umsetzung von Notfallplänen für Sicherheitsvorfälle bei personenbezogenen Informationen und andere Maßnahmen gemäß den Gesetzen und Vorschriften.[19]

Praktische Bedeutung für Einrichtungen in Deutschland

Falls personenbezogene Daten wie z. B. im Zusammenhang mit dem Austausch von Studierenden oder Forschenden für das Projekt relevant sind, sollten die Einrichtungen in Deutschland die Einhaltung durch die Beachtung der oben genannten Bestimmungen unterstützen. Im Falle von anonymisierten personenbezogenen Informationen, bei denen die Identität einer natürlichen Person nicht direkt bestimmt werden kann wie z. B. anonymisierte personenbezogene Informationen in einem Forschungsprojekt, ist die Datenübermittlung in der Regel unproblematisch, es sei denn, die Daten unterliegen anderen Einschränkungen, wenn sie z. B. als wichtige Daten gelten.

17 Artikel 55 PIPL.
18 Artikel 38 PIPL.
19 Artikel 51 PIPL.

3.2 Bestimmungen zur Förderung und Regulierung des grenzüberschreitenden Datenverkehrs (CBDF-Bestimmungen) (2024)

Die CBDF-Bestimmungen sind seit dem 22. März 2024 in Kraft und enthalten bestimmte Liberalisierungen hinsichtlich der grenzüberschreitenden Datenübermittlung. Die wichtigste zuständige Behörde ist die CAC.

Zur Beteiligung von Treuhandeinrichtungen, einschließlich „wissenschaftlicher Datenzentren" siehe 3.3.

Die CBDF-Bestimmungen legen **sechs Fälle fest, in denen Datenverarbeiter von der Verpflichtung befreit sind**, eine Sicherheitsbewertung für die grenzüberschreitende Datenübermittlung durchzuführen, einen Standardvertrag für die Übermittlung personenbezogener Informationen ins Ausland abzuschließen oder eine Zertifizierung zum Schutz personenbezogener Informationen vorzunehmen:

(i) Daten, bei denen es sich weder um personenbezogene Informationen noch um wichtige Daten (wie im DSL und den NDSM-Bestimmungen definiert, siehe 3.5) handelt, die im Rahmen des internationalen Handels, des grenzüberschreitenden Transports, der **akademischen Zusammenarbeit**, der grenzüberschreitenden Produktion und Herstellung, des Marketings und der Werbung erhoben oder erstellt werden.

(ii) Personenbezogene Informationen (mit Ausnahme sensibler personenbezogener Informationen gemäß der Definition im PIPL, siehe 3.1) von **weniger als 100.000 Personen**, die im Zeitraum ab dem 1. Januar eines bestimmten Jahres übermittelt werden.

(iii) Personenbezogene Informationen, **die ursprünglich im Ausland gesammelt oder generiert** wurden und dann nach China transferiert und dort verarbeitet werden, ohne dass personenbezogene Informationen oder wichtige Daten, die vor dem Re-Export in China generiert wurden, hinzugefügt werden.

(iv) Personenbezogene Informationen einschließlich sensibler personenbezogener Informationen, die für den Abschluss und die Erfüllung eines Vertrages für eine natürliche Person als Vertragspartner erforderlich sind, wie z. B. für grenzüberschreitende Einkäufe, Lieferdienste, Überweisungen, Zahlungen, Kontoeröffnungen, Flugticket- und Hotelreservierungen, Visumanträge und **Prüfungsdienstleistungen**.

(v) Personenbezogene Informationen einschließlich sensibler personenbezogener Informationen interner Mitarbeiterinnen und Mitarbeiter zur Umsetzung des Personalmanagements im Ausland, in Übereinstimmung mit den arbeitsrechtlichen Vorschriften und den gemäß dem Gesetz unterzeichneten Tarifverträgen.

(vi) Personenbezogene Informationen einschließlich sensibler personenbezogener Informationen, die in einem Notfall übermittelt werden müssen, um das Leben, die Gesundheit oder das Eigentum von natürlichen Personen zu schützen.

Die Ausnahmeregelung in Punkt (i) oben kann im Falle einer Forschungskooperation von besonderer Bedeutung sein. Voraussetzung für die Ausnahmeregelung ist, dass es sich nicht um personenbezogene Informationen handelt (siehe 3.1), und dass keine wichtigen Daten betroffen sind (siehe 3.5).

Falls personenbezogene Informationen im Rahmen eines grenzüberschreitenden Forschungsprojekts nach China übermittelt werden, ist eine Wiederausfuhr der Daten unter Punkt (iii) oben ausgenommen, unter der Voraussetzung, dass keine weiteren personenbezogenen Informationen (siehe 3.1) oder wichtige Daten (siehe 3.5), die in China generiert wurden, hinzugefügt werden.

Ein Vertrag über Prüfungsleistungen zwischen chinesischen Studierenden und einer Einrichtung in Deutschland ist unter Punkt (iv) oben ausgenommen.

Die CBDF-Bestimmungen **verlangen ausdrücklich die folgenden Bedingungen** für die grenzüberschreitende Übermittlung von Daten je nach den Umständen der Datenübermittlung:

(i) **Eine Sicherheitsbewertung** durch die CAC ist erforderlich:
- wenn Betreiber kritischer Informationsinfrastrukturen (CII-Betreiber, siehe **3.4**) personenbezogene Informationen oder wichtige Daten an das Ausland weitergeben (siehe unter CSL oben); oder
- wenn Datenverarbeiter, die keine CII-Betreiber sind, wichtige Daten nach Übersee übermitteln oder ab dem 1. Januar eines bestimmten Jahres personenbezogene Informationen (mit Ausnahme sensibler personenbezogener Informationen) von mehr als 1 Million Menschen oder sensible personenbezogene Informationen von mehr als 10.000 Menschen insgesamt nach Übersee übermitteln.

(ii) **Die Zertifizierung durch eine spezialisierte Agentur / ein Standardvertrag** mit dem Empfänger in Übersee und die Einreichung von Unterlagen beim CAC sind erforderlich:
- wenn die Einrichtung kein CII-Betreiber ist; und
- bei der Übermittlung personenbezogener Informationen (mit Ausnahme sensibler personenbezogener Informationen) von mehr als 100.000, aber weniger als 1 Million Personen im Ausland insgesamt seit dem 1. Januar eines bestimmten Jahres; oder
- bei der Bereitstellung sensibler personenbezogener Informationen von weniger als 10.000 Personen im Ausland insgesamt seit dem 1. Januar eines bestimmten Jahres.

Praktische Bedeutung für Einrichtungen in Deutschland

Einrichtungen in Deutschland sollten sich sowohl der Möglichkeit bewusst sein, dass bestimmte Daten in manchen Fällen frei grenzüberschreitend übermittelt werden können, als auch der Fälle, in denen eine Sicherheitsüberprüfung durch die CAC, eine Zertifizierung durch eine spezialisierte Agentur / ein Standardvertrag mit dem ausländischen Empfänger nach den CBDF-Bestimmungen ausdrücklich erforderlich sind. Durch die **Aufnahme einer Standardklausel** in den Kooperationsvertrag, siehe **4.1**, kann die deutsche Institution proaktiv vor der Datenübermittlung einen Nachweis über die Einhaltung der Bestimmungen verlangen.

3.3 Maßnahmen für die Verwaltung von wissenschaftlichen Daten (ASD-Maßnahmen) (2018)

Die ASD-Maßnahmen sind seit dem 17. März 2018 in Kraft. Die wichtigste zuständige Behörde ist das Ministerium für Wissenschaft und Technologie (**MOST**).

Die ASD-Maßnahmen gelten für Aktivitäten im Zusammenhang mit wissenschaftlichen Daten, einschließlich deren Sammlung und Produktion, Verarbeitung und Aussortierung, Öffnung und Weitergabe sowie Verwaltung und Nutzung, die mit Unterstützung von Haushaltsmitteln der Regierung durchgeführt werden.

In China sind die **zuständigen wissenschaftlichen Forschungsinstitute, Hochschulen, Unternehmen und andere juristische Personen die verantwortlichen Stellen** für die Verwaltung wissenschaftlicher Daten. Sie nehmen die folgenden Hauptaufgaben wahr:

(i) die Umsetzung der nationalen und regionalen Politik für die Verwaltung wissenschaftlicher Daten und Aufbau eines soliden Verwaltungssystems für die jeweiligen wissenschaftlichen Daten;
(ii) die Sammlung und Erstellung, Verarbeitung und Anordnung sowie die langfristige Speicherung wissenschaftlicher Daten gemäß den einschlägigen Standardspezifikationen, um die Datenqualität zu gewährleisten;
(iii) die ordnungsgemäße vertrauliche Behandlung und Sicherheitsverwaltung wissenschaftlicher Daten gemäß den einschlägigen Bestimmungen;
(iv) die Einrichtung eines Systems zur Verwaltung wissenschaftlicher Daten, die Bekanntgabe des frei zugänglichen Katalogs für wissenschaftliche Daten und dessen rechtzeitige Aktualisierung sowie die aktive Bereitstellung eines Dienstes zur gemeinsamen Nutzung wissenschaftlicher Daten;
(v) die Gewährleistung von Hardware- und Software-Einrichtungen und anderen Bedingungen, Mitteln und Personal, die für die Verwaltung und den Betrieb wissenschaftlicher Daten erforderlich sind.[20]

Wissenschaftliche Datenzentren sollen als wichtige Träger zur Förderung der Öffnung und gemeinsamen Nutzung wissenschaftlicher Daten mit folgenden Hauptaufgaben eingerichtet werden:

(i) die Integration und Vorlage wissenschaftlicher Daten in den relevanten Bereichen;
(ii) die Übernahme der hierarchischen Klassifizierung, der Verarbeitung und Sortierung sowie der Analyse und Auswertung wissenschaftlicher Daten;
(iii) die Gewährleistung der Sicherheit wissenschaftlicher Daten und die Förderung der Öffnung und des Austauschs wissenschaftlicher Daten, wie es die Gesetze und Vorschriften vorsehen;
(iv) die Stärkung des Austauschs und der Zusammenarbeit im Bereich wissenschaftlicher Daten sowohl auf nationaler als auch auf internationaler Ebene.[21]

DEFINITION

Wissenschaftliche Daten sind definiert als Daten, die aus der Grundlagenforschung, der Anwendungsforschung, der Pilotentwicklung und anderen Bereichen wie den Naturwissenschaften und Ingenieurwissenschaften stammen, sowie die Originaldaten und abgeleitete Daten, die durch Beobachtung und Überwachung, Erhebung und Untersuchung sowie Inspektion und Detektion gewonnen und für wissenschaftliche Forschungsaktivitäten verwendet werden.[22]

20 Artikel 9 ASD-Maßnahmen.
21 Artikel 10 ASD-Maßnahmen.
22 Artikel 2 ASD-Maßnahmen.

DEFINITION

Ein Staatsgeheimnis ist definiert als eine Angelegenheit, die für die nationale Sicherheit und die nationalen Interessen von entscheidender Bedeutung ist und die gemäß den gesetzlichen Bestimmungen nur einem begrenzten Personenkreis für einen bestimmten Zeitraum zugänglich gemacht wird.[23] Zu den Staatsgeheimnissen gehören Verschlusssachen aus Wissenschaft und Technik, die die nationale Sicherheit und die nationalen Interessen betreffen und deren Bekanntwerden die nationale Sicherheit und die nationalen Interessen in den Bereichen Politik, Wirtschaft, Landesverteidigung, Außenpolitik usw. gefährden kann.

Zum Umgang mit staatlichen Daten im Rahmen anderer Vorschriften siehe **3.3** unten.

Wissenschaftliche Daten, die im Rahmen eines mit staatlichen Mitteln geförderten wissenschaftlichen und technologischen Projekts auf einer beliebigen Ebene gewonnen wurden, müssen dem entsprechenden wissenschaftlichen Datenzentrum vorgelegt werden. Wenn eine Abhandlung auf der Grundlage von wissenschaftlichen Daten verfasst wird, die mit Hilfe staatlicher Mittel gewonnen wurden, und die **Veröffentlichung der Abhandlung in einer ausländischen wissenschaftlichen Zeitschrift** die Vorlage der entsprechenden wissenschaftlichen Daten erfordert, muss die Autorin oder der Autor der Abhandlung die wissenschaftlichen Daten vor der Veröffentlichung der Arbeitgeberin oder dem Arbeitgeber zur einheitlichen Verwaltung vorlegen. Für wissenschaftliche Daten, die mit Unterstützung nichtöffentlicher Gelder gewonnen wurden und Staatsgeheimnisse, die Staatssicherheit oder soziale öffentliche Interessen betreffen, gelten besondere Regeln.[24]

Wissenschaftliche Daten, die ein Staatsgeheimnis, die Sicherheit des Staates, öffentliche Interessen, Geschäftsgeheimnisse oder den Schutz der Privatsphäre betreffen, dürfen grundsätzlich nicht offengelegt und weitergegeben werden. Wenn Offenheit erforderlich ist, prüfen die zuständigen Stellen den Zweck, die Qualifikation der Nutzenden, die Bedingungen der Vertraulichkeit und andere Faktoren und kontrollieren den Umfang der Informationen.

Wenn wissenschaftliche Daten, die ein Staatsgeheimnis berühren, **im Rahmen der Kommunikation und Zusammenarbeit mit dem Ausland** zur Verfügung gestellt werden müssen, legt die zuständige Stelle die Kategorie, den Umfang und den Zweck der zu verwendenden Daten fest und meldet den Fall der zuständigen Behörde zur Genehmigung im Rahmen der vorgeschriebenen Verfahren zur Verwaltung der Vertraulichkeit. Nach der Genehmigung führt die zuständige Stelle die entsprechenden Verfahren durch und schließt eine Vertraulichkeitsvereinbarung mit der Datennutzerin oder dem Datennutzer ab.[25] Die Transparenz kann durch Hinzufügen einer **entsprechenden Klausel** erhöht werden, siehe **4.1**.

Der Standard GB/T 39912-2021 (Archivierung wissenschaftlicher Daten aus Wissenschafts- und Technologieprogrammen – Technische und verwaltungstechnische Spezifikation) legt die Grundsätze der Übertragung wissenschaftlicher Daten aus Wissenschafts- und Technologieprojekten, die wichtigsten Verwaltungsorgane und Verantwortlichkeiten sowie die wichtigsten Inhalte und Verfahren fest. Dieser Standard gilt für den Transfer und die Verwaltung wissenschaftlicher Daten bei allen Arten

23 Artikel 2 des *Gesetzes zur Wahrung von Staatsgeheimnissen* (2024).

24 Artikel 14, 15 ASD-Maßnahmen.

25 Artikel 26 ASD-Maßnahmen.

von Wissenschafts- und Technologieprojekten auf allen Ebenen, **die mit staatlichen Mitteln finanziert werden**. Für den Transfer und die Verwaltung wissenschaftlicher Daten von Wissenschafts- und Technologieprojekten, die auf andere Weise verwaltet werden, kann dieser Standard als Referenz dienen. Er ist der spezifische nationale Standard zur Regelung wissenschaftlicher Daten und spiegelt die gleichen Anforderungen wie die ASD-Maßnahmen wider. Bezüglich eines zusätzlichen nationalen Standards zur Klassifizierung und Einstufung von Daten siehe **3.5**.

Praktische Bedeutung für Einrichtungen in Deutschland
Die Einrichtungen in Deutschland sollten hinsichtlich der oben genannten Vorschriften sensibel sein. Es ist wichtig zu wissen, ob wissenschaftliche Daten mit Unterstützung der chinesischen Regierung erstellt wurden. **Die Veröffentlichung in ausländischen Fachzeitschriften sowie der Datenexport im Rahmen der Auslandskommunikation und -kooperation unterliegt den Beschränkungen der ASD-Maßnahmen**. Die Unterstützung der Einhaltung durch die Einrichtung in Deutschland kann durch die Standardklausel klar geregelt werden.

3.4 Gesetz zur Cybersicherheit (CSL) (2017)

Das CSL ist seit dem 1. Juni 2017 in Kraft. Die wichtigsten zuständigen Behörden im Rahmen des CSL sind wieder CAC und PSB.

Das CSL sieht ein **mehrstufiges Schutzsystem (MLPS)** für die Netzwerksicherheit vor.[26]

Zwei empfohlene nationale Standards, nämlich **GB/T 22240-2020** (Informationssicherheitstechnologie – Klassifizierungsleitfaden für den klassifizierten Schutz der Cybersicherheit) und **GB/T 22239-2019** (Informationssicherheitstechnologie – Grundlage für den klassifizierten Schutz der Cybersicherheit) bieten detaillierte technische Standards für die Bestimmung des Schutzniveaus sowie die Anforderungen an die Einhaltung der jeweiligen Stufen.[27]

Das CSL umreißt die gesetzlichen **allgemeinen Verpflichtungen zur Netzsicherheit für Netzbetreiber:**

(i) Formulierung interner Sicherheitsmanagementsysteme und Betriebsanweisungen, um die für die Cybersicherheit verantwortliche Person zu bestimmen und die Verantwortlichkeit für die Cybersicherheit festzulegen;
(ii) Ergreifung technischer Maßnahmen zur Verhinderung von Computerviren, Netzwerkangriffen, Netzwerkeinbrüchen und anderen Aktivitäten, die die Cybersicherheit gefährden;
(iii) Ergreifung technischer Maßnahmen zur Überwachung und Aufzeichnung des Netzwerkbetriebs und von Cybersecurity-Ereignissen und Aufbewahrung der cyberbezogenen Protokolle für mindestens sechs Monate wie vorgeschrieben;

26 Artikel 21 CSL; Siehe auch den Entwurf der *Verordnungen über den abgestuften Schutz für Cybersicherheit*, der am 27. Juni 2018 zur öffentlichen Stellungnahme veröffentlicht wurde.

27 Obwohl diese beiden Standards nicht verbindlich sind, werden sie von den Sicherheitsbehörden als verbindlich angesehen. In der Praxis muss jeder Netzbetreiber in China die Anforderungen dieser beiden Standards einhalten. Auf der Grundlage der Vorschriften für MLPS können die Netzwerksysteme jedes Netzwerkbetreibers in verschiedene Stufen eingeteilt werden. Die nationalen Standards enthalten detaillierte Sicherheitsanforderungen für jede Stufe. Diese Anforderungen bestehen aus zwei Hauptaspekten, die die physische Umgebung, die Kommunikations- und Computersicherheit sowie das Sicherheitsmanagement, die Organisation und das Personal usw. betreffen. Die MLPS verlangt eine Selbsteinstufung in eine der fünf Stufen, während ab Stufe 2 auch eine Registrierung bei der lokal zuständigen PSB erforderlich ist.

(iv) Ergreifung von Maßnahmen wie Datenklassifizierung, Sicherung und Verschlüsselung wichtiger Daten usw. sowie Erfüllung anderer in Gesetzen und Vorschriften vorgesehener Verpflichtungen.[28]
(v) Ausarbeitung eines Notfallplans zur sofortigen Reaktion auf Sicherheitsrisiken wie Systemfehler, Computerviren, Netzwerkangriffe und Eindringlinge.[29]
(vi) Einrichtung von Beschwerde- und Meldemechanismen für die Informationssicherheit im Netz.[30]
(vii) Schutz der personenbezogenen Informationen von Einzelpersonen.[31]

Einrichtungen in Deutschland sollten entsprechend sensibel sein, z. B. wenn Forschungsprojekte eine oder mehrere der oben genannten Industrien oder Sektoren betreffen.Beispielsweise umfasst das Projekt Daten zur vorbeugenden Wartung von Windkraftanlagen (mit Bezug zu „Energie"). Eine Klausel könnte in die entsprechende(n) Vereinbarung(en) aufgenommen werden, siehe **4.1**.

Ein CII-Betreiber muss **besondere gesetzliche Sicherheitsverpflichtungen** erfüllen, einschließlich der Einrichtung von Sicherheitsmanagementgremien, der Durchführung von Personen- und Sicherheitsüberprüfungen, der Gewährleistung von Cybersicherheitsschulungen, der Pflege von Notfallwiederherstellungsplänen, des Schutzes von Daten in China und der Durchführung von Bewertungen vor der grenzüberschreitenden Übertragung von personenbezogenen Informationen und wichtigen Daten (gemäß der Definition unter **3.1** und **3.5**).[32]

DEFINITION

Kritische Informationsinfrastrukturen (CII) werden definiert als Informationsinfrastrukturen in wichtigen Branchen und Sektoren wie öffentliche Kommunikation, Informationsdienste, Energie, Verkehr, Wasserwirtschaft, Finanzen, öffentlicher Dienst und elektronische Behördendienste sowie andere kritische Informationsinfrastrukturen, die im Falle einer Beschädigung, Deaktivierung oder Offenlegung von Daten die nationale Sicherheit, die Volkswirtschaft, den Lebensunterhalt der Menschen und die öffentlichen Interessen ernsthaft gefährden können.[33]

28 Artikel 21 CSL.

29 Artikel 25 CSL.

30 Artikel 49 CSL.

31 Artikel 40-45 CSL.

32 Artikel 34-37 CSL:
(i) die Einrichtung eines speziellen Gremiums für das Sicherheitsmanagement und die Benennung einer verantwortlichen Person sowie die Überprüfung des Sicherheitshintergrunds der genannten Person und der Personen in Schlüsselpositionen;
(ii) die Bereitstellung von regelmäßiger Cybersicherheitsschulung, technischem Training und einer Bewertung der Fähigkeiten von Praktikerinnen und Praktikern;
(iii) Erstellung von Sicherungskopien wichtiger Systeme und Datenbanken für den Notfall;
(iv) einen Notfallplan für Cybersicherheitsvorfälle ausarbeiten und regelmäßig Übungen durchführen;
(v) die Erfüllung anderer Verpflichtungen, die in Gesetzen und Vorschriften vorgesehen sind;
(vi) **Sicherheitsüberprüfung** durch das CAC beim Kauf von Netzwerkprodukten und -dienstleistungen, die die nationale Sicherheit gefährden könnten, und Abschluss von Geheimhaltungsvereinbarungen mit dem Produkt-/Dienstleistungsanbieter;
(vii) **Speicherung von personenbezogenen Informationen und wichtigen Daten**, die während einer Tätigkeit in China gesammelt und generiert wurden, innerhalb des chinesischen Hoheitsgebiets; Bestehen einer **Sicherheitsüberprüfung durch die CAC**, bevor personenbezogene Informationen oder wichtige Daten ins Ausland übermittelt werden.

33 Artikel 31 CSL.

Praktische Bedeutung für Einrichtungen in Deutschland
Die Einrichtungen in Deutschland sollten hinsichtlich der oben genannten Vorschriften sensibel sein. Es ist wichtig zu verstehen

(i) **ob eine chinesische Kooperationseinrichtung ein CII-Betreiber** ist oder das Projekt einen CII-Betreiber einbezieht, und/oder
(ii) **ob wichtige Daten betroffen sind**.

Die Einrichtungen in Deutschland sollten die chinesischen Kooperationspartner auffordern, die notwendigen Maßnahmen und Verfahren im Voraus zu klären; eine **entsprechende Klausel** kann hinzugefügt werden, wie in **4.1** vorgeschlagen. Wenn ein CII-Betreiber und/oder wichtige Daten betroffen sind, sollte die deutsche Einrichtung die Einhaltung unterstützen. **Das CSL verpflichtet nur den CII-Betreiber selbst**, die strengen Compliance-Regeln in Bezug auf Cybersicherheit und Datenschutz zu befolgen. Für wichtige Daten sind im DSL weitere Compliance-Regeln festgelegt (siehe **3.5**).

Das CSL wurde am 28. Oktober 2025 vom Ständigen Ausschuss des Nationalen Volkskongresses geändert und trat am 1. Januar 2026 in Kraft. Die wichtigsten Änderungen sind wie folgt:

Es wird ausdrücklich festgelegt, dass der Staat die Grundlagenforschung im Bereich der künstlichen Intelligenz und die Entwicklung von Schlüsseltechnologien wie Algorithmen unterstützen, den Aufbau von Infrastruktur einschließlich Trainingsdatenressourcen und Rechenleistung vorantreiben, ethische Standards für künstliche Intelligenz verfeinern, die Risikoüberwachung, -bewertung und Sicherheitsaufsicht verstärken sowie die Anwendung und gesunde Entwicklung künstlicher Intelligenz fördern soll.

Es wird betont, dass die Übereinstimmung mit dem Cybersicherheitsgesetz, dem Zivilgesetzbuch der Volksrepublik China und dem Gesetz zum Schutz personenbezogener Daten der Volksrepublik China gewährleistet sein muss.

Die Strafmechanismen für die Nichteinhaltung von Cybersicherheitsverpflichtungen werden verfeinert, einschließlich der Umstände, die eine Erhöhung der Strafen rechtfertigen, sowie der Umstände, die gemäß dem Gesetz über Verwaltungsstrafen eine Strafmilderung, eine Strafminderung oder eine Befreiung von Strafen rechtfertigen.

Der Umfang der Sanktionen gegen eine ausländische Einheit, die Aktivitäten ausübt, die die Cybersicherheit Chinas gefährden, wird erweitert.

Praktische Bedeutung für Einrichtungen in Deutschland
Wenn die Einrichtungen in Deutschland Aktivitäten ausüben, die die Cybersicherheit der Volksrepublik China gefährden und diese schwerwiegende Folgen haben, können die zuständigen Behörden Maßnahmen wie das Einfrieren von Vermögenswerten oder andere notwendige Sanktionen gegen die ausländische Einrichtung verhängen. Daher sollten Einrichtungen in Deutschland Verstöße gegen das Cybersicherheitsgesetz vermeiden.

3.5 Datenschutzgesetz (DSL) (2021)

Das DSL ist seit dem 1. September 2021 in Kraft. Die wichtigsten zuständigen Behörden im Rahmen des DSL sind hauptsächlich die CAC und verschiedene Ministerien der Zentralregierung.

Das DSL sieht ein **System zur Klassifizierung und zum hierarchischen Schutz von Daten** vor, um die Daten je nach ihrer Bedeutung für die wirtschaftliche und soziale Entwicklung und dem Schaden für die nationale Sicherheit, die öffentlichen Interessen oder die legitimen Rechte und Interessen von Einzelpersonen und Organisationen zu schützen, wenn die Daten gefälscht, beschädigt, weitergegeben, unrechtmäßig erlangt oder unrechtmäßig verwendet werden.

Kerndaten des Staates, die die nationale Sicherheit, die Lebensgrundlagen der nationalen Wirtschaft, die Lebensgrundlagen wichtiger Menschen, wichtige öffentliche Interessen usw. betreffen, unterliegen einem strengeren Verwaltungssystem.

Kataloge, in denen wichtige Daten definiert werden, die nicht im DSL aufgeführt sind, werden von den jeweiligen lokalen Regierungen und Ministerien als zuständige Behörden für die jeweiligen Industrien und Wirtschaftszweige formuliert. Mit Ausnahme der Automobilindustrie und der Pilot-Freihandelszonen in Tianjin, Peking und Shanghai sind die entsprechenden Kataloge jedoch noch in der Diskussion und bisher nicht veröffentlicht. Insbesondere die erste gemeinsame Negativliste für die Freihandelszone China (Shanghai) und die Lingang New Area, die am 8. Februar 2025 veröffentlicht wurde, deckt derzeit nur drei Schlüsselbereiche ab: Finanzen (Rückversicherung), Schifffahrt (internationale Schifffahrt) und Handel (Einzelhandel und Gastronomie, Beherbergung). Der nationale Standard **GB/T 43697-2024** (Datensicherheitstechnologie – Regeln für die Klassifizierung und Einstufung von Daten), der seit dem 1. Oktober 2024 in Kraft ist, enthält allgemeine Regeln für Datenverarbeiter zur Identifizierung **wichtiger Daten.**

DEFINITION

Wichtige Daten werden im DSL und den NDSM-Bestimmungen als Daten in einem bestimmten Bereich, einer bestimmten Gruppe oder Region oder mit einer bestimmten Genauigkeit und einem bestimmten Umfang definiert, die, wenn sie manipuliert, zerstört, weitergegeben, unrechtmäßig erlangt oder unrechtmäßig verwendet werden, die nationale Sicherheit, den wirtschaftlichen Betrieb, die soziale Stabilität, die öffentliche Gesundheit und Sicherheit direkt gefährden können. Weitere Einzelheiten zu wichtigen Daten sind für verschiedene Regionen und Abteilungen, Branchen usw. festzulegen (siehe **3.8.3**). Die NDSM-Bestimmungen besagen jedoch, dass für Daten, die nicht von der jeweiligen Region oder Abteilung oder anderweitig öffentlich als wichtige Daten bekannt gegeben wurden, keine Sicherheitsbewertung für die grenzüberschreitende Übermittlung solcher Daten erforderlich ist. Andere (auch künftige) Gesetze, Verordnungen und Standards können weitere Definitionen enthalten, die von den oben genannten abweichen oder diese ergänzen können.
Die Pilot-Freihandelszonen sind berechtigt, ihre eigenen Listen für wichtige Daten oder allgemeine Daten zu definieren. Bislang haben die Pilot-Freihandelszonen in Tianjin, Peking und Shanghai (einschließlich Lingang) entsprechende Negativlisten für wichtige Daten herausgegeben, während die Pilot-Freihandelszone in Shanghai Lingang eine Positivliste für drei Branchen veröffentlicht hat, darunter für intelligente Fahrzeuge, biomedizinische Produkte und Public Offering Fonds.

Dieser nationale Standard kann von Einrichtungen in China als Referenz verwendet werden, ist aber noch weit von einem umsetzbaren branchenbasierten Katalog wichtiger Daten entfernt. Die zentrale Herausforderung liegt in den zu weit gefassten Definitionen und der mangelnden Spezifität. Durch die Verwendung von „catch all"-Klauseln, die sich potenziell auf fast jeden kritischen Sektor auswirken – von der nationalen Sicherheit bis hin zur Raumfahrt und KI – werden Datenverarbeitende dieses Standards ohne klare Grenzen oder branchenspezifische Richtlinien zurückgelassen. Dies verdeutlicht das **Spannungsverhältnis zwischen der Gewährleistung von Flexibilität** bei der Bewältigung sich entwickelnder Sicherheitsbedrohungen **und der Bereitstellung praktischer, umsetzbarer Leitlinien** für die Einhaltung der Vorschriften.

Gemäß dem DSL muss der Verarbeiter von Daten die folgenden **allgemeinen Datenschutzverpflichtungen** einhalten:

(i) die Einrichtung eines soliden Systems zur Verwaltung der Datensicherheit während des gesamten Prozesses;
(ii) die Organisation von Datensicherheitsschulungen und -trainings, und
(iii) das Ergreifen entsprechender technischer und sonstiger notwendiger Maßnahmen zur Gewährleistung der Datensicherheit.[34]

Gemäß dem DSL muss der **Verarbeiter wichtiger Daten** die folgenden zusätzlichen Verpflichtungen erfüllen:
(i) die Angabe der für die Datensicherheit verantwortlichen Person und des Verwaltungsorgans sowie die Durchführung der Maßnahmen zum Schutz der Daten;[35]
(ii) die regelmäßige Durchführung einer Risikobewertung der Datenverarbeitungstätigkeiten;[36]
(iii) die Durchführung der Sicherheitsbewertung im Falle des Exports wichtiger Daten.[37]

Praktische Bedeutung für Einrichtungen in Deutschland
Die Einrichtungen in Deutschland sollten hinsichtlich der oben genannten Vorschriften sensibel sein. Es ist besonders relevant zu verstehen, ob es sich um wichtige Daten im Sinne der chinesischen Gesetze und Vorschriften handelt. **Im Zweifelsfall** sollte die deutsche Einrichtung eine spezialisierte externe Beraterin oder einen spezialisierten externen Berater konsultieren, z. B. eine Anwaltskanzlei, die weitere Hinweise geben kann. Auch eine **entsprechende Klausel** kann zur Erhöhung der Transparenz beitragen, siehe **4.1**. Dies kann z. B. (i) Verbesserungen in der Datenverwaltung, der Aus- und Weiterbildung des Personals, (ii) technische Maßnahmen, (iii) die Festlegung der verantwortlichen Personen und (iv) die Durchführung von Risikobewertungen umfassen.

34 Artikel 27 DSL.
35 Artikel 27 DSL.
36 Artikel 30 DSL.
37 Artikel 31 DSL.

3.6 Ausfuhrkontrollgesetz (ECL) (2020)

Das ECL ist seit dem 1. Dezember 2020 in Kraft. Auf der Grundlage des ECL ist *die Verordnung der Volksrepublik China über die Exportkontrolle von Gütern mit doppeltem Verwendungszweck* seit dem 1. Dezember 2024 in Kraft. Die zuständige Behörde ist hauptsächlich das Handelsministerium (**MOFCOM**).

Die Definitionen in Europa und China haben den Kerngedanken des doppelten Verwendungszwecks sowie den Bezug auf Waffen und Technologien gemeinsam und umfassen Waren, immaterielle Güter wie Technologien, und Dienstleistungen. Innerhalb Chinas unterliegt auch die Lieferung an eine ausländische Person (z. B. an ausländische Forschenden) der Exportkontrolle. Während sich die chinesische Definition von Dual-Use eher auf militärisches Potenzial und Massenvernichtungswaffen konzentriert, ist die europäische Definition[38] weiter gefasst.

Das MOFCOM aktualisiert regelmäßig die **Kontrollliste** der Waren und Dienstleistungen auf der offiziellen Website (http://exportcontrol.mofcom.gov.cn/). Außerdem kann es zu einer vorübergehenden Kontrolle von Gütern, Technologien und Dienstleistungen kommen, die nicht in der Exportkontrollliste aufgeführt sind. Die Dauer der vorübergehenden Kontrolle darf zwei Jahre nicht überschreiten. Exporteure von kontrollierten Gütern oder vorübergehend kontrollierten Gütern müssen beim MOFCOM **eine Ausfuhrgenehmigung** beantragen.[39]

DEFINITION

Unter kontrollierten Gütern versteht man z. B. militärische Produkte, nukleare und andere Güter, Technologien, Dienstleistungen und Gegenstände, die sich auf die Wahrung der nationalen Sicherheit beziehen. Dazu gehören auch technische Informationen und Daten im Zusammenhang mit diesen Gütern.

DEFINITION

Güter mit doppeltem Verwendungszweck sind definiert als Güter, Technologien und Dienstleistungen, die sowohl für zivile als auch für militärische Zwecke verwendet werden können oder die zur Steigerung des militärischen Potenzials beitragen, insbesondere solche, die für die Konstruktion, Entwicklung, Herstellung oder den Einsatz von Massenvernichtungswaffen und deren Trägermitteln verwendet werden können.[40]

Praktische Bedeutung für Einrichtungen in Deutschland

Die Einrichtungen in Deutschland und die deutschen Forschenden in China sollten die oben genannten Vorschriften aufmerksam verfolgen. Es ist wichtig zu verstehen, ob Produkte, Dienstleistungen oder Technologien als kontrollierte Güter oder als Güter mit doppeltem Verwendungszweck eingestuft werden können, um die Einhaltung des ECL sicherzustellen.

38 Artikel 2(1), Regulation 2021/821: https://eur-lex.europa.eu/eli/reg/2021/821/oj/eng.

39 Artikel 12 ECL.

40 Artikel 2 ECL.

3.7 Gesetz zur Spionageabwehr (CEL) (2023)

Das CEL ist seit dem 1. Juli 2023 in Kraft. Es gibt Berichte über eine kleine Anzahl ausländischer Personen oder ausländisch investierte Einrichtungen, die unter dem CEL sanktioniert wurden. **In der allgemeinen Rechts- und Unternehmenspraxis in China spielt das CEL jedoch bisher keine große Rolle**, obwohl es in den Medien große Beachtung findet. Relevant für den Forschungskontext: Der Schutz von Staatsgeheimnissen und der Staatssicherheit wird in den ASD-Maßnahmen bereits seit 2018 angesprochen (siehe oben 3.3). **Die geforderte Einhaltung der ASD-Maßnahmen in Bezug auf Staatsgeheimnisse und die Sicherheit des Staates betreffende wissenschaftliche Daten verringert potenzielle Risiken auch im Rahmen des CEL.** Die wichtigsten zuständigen Behörden sind das Ministerium für Staatssicherheit (MSS) und die lokalen PSB.

Ein Verstoß gegen das CEL kann zu administrativen Sanktionen wie Verwarnungen, Festnahmen, Geldstrafen für die betroffenen Personen oder Einrichtungen und im schlimmsten Fall zu einer strafrechtlichen Haftung führen.[41]

DEFINITION

Spionage ist laut CEL definiert als:

(i) Aktivitäten, die die nationale Sicherheit Chinas gefährden, begangen von einer Spionageorganisation, ihren Agentinnen oder Agenten oder einer anderen Person, die von einer solchen Organisation oder einer solchen Agentin oder einem solchen Agenten angestiftet/finanziert wird/mit ihr/ihm gemeinsame Sache macht (gemeinsam bezeichnet als **Spionin oder Spion**);

(ii) Beitritt zu einer Spionageorganisation oder Annahme eines Auftrags, der von einer Spionageorganisation oder ihrer Agentin oder ihrem Agenten erteilt wurde, oder Überlaufen zu einer Spionageorganisation oder ihrer Agentin oder ihrem Agenten;

(iii) Diebstahl, Ausforschen, Kauf oder illegale Weitergabe von Staatsgeheimnissen, nachrichtendienstlichen oder anderen Dokumenten, Daten, Materialien oder Artikeln, die sich auf die nationale Sicherheit oder nationale Interessen beziehen, oder Anstiftung, Verlockung, Nötigung oder Bestechung einer Mitarbeiterin oder eines Mitarbeiters des Staates zum Überlaufen;

(iv) Cyberangriffe, Eindringen, Beeinflussung, Kontrolle oder Zerstörung gegen ein staatliches Organ, eine geheimhaltungsrelevante Einrichtung oder eine CII usw., die von einer Spionin oder einem Spion begangen werden;

(v) Anzeige von Angriffszielen für Feinde; und

(vi) andere Spionageaktivitäten.[42]

41 Artikel 53 CEL.

42 Artikel 4 CEL.

Praktische Bedeutung für Einrichtungen in Deutschland
Einrichtungen in Deutschland sollten sensibel mit den verbotenen Spionageaktivitäten umgehen, aber auch die Risiken bei jedem einzelnen Kooperationsprojekt vernünftig bewerten. Insbesondere die ohnehin geforderte Einhaltung der zuvor verabschiedeten ASD-Maßnahmen in Bezug auf Staatsgeheimnisse und wissenschaftliche Daten mit Bezug zur Staatssicherheit (siehe oben **3.3**) verringert potenzielle Risiken auch unter dem CEL. Je proaktiver Einrichtungen in Deutschland mit ihren chinesischen Kolleginnen und Kollegen und den chinesischen Behörden interagieren, **indem sie alle Bedenken offen ansprechen, idealerweise schriftlich und im Voraus**, desto geringer ist das Risiko späterer potenzieller Vorwürfe. Compliance-Maßnahmen, die unter Berücksichtigung anderer Gesetze wie PIPL, CSL, DSL und ECL ergriffen werden, können dieses Risiko ebenfalls verringern.

3.8 Andere Sonderregelungen

Die nachstehenden Regelungen können nur in Einzelfällen relevant sein und werden der Vollständigkeit halber aufgeführt.

3.8.1 Verwaltungsvorschriften über humangenetische Ressourcen (HGR-Vorschriften)

Die HGR-Vorschriften wurden vom Staatsrat am 28. Mai 2019 verkündet und am 10. März 2024 überarbeitet. Die Nationale Gesundheitskommission (**NHC**) ist landesweit für die Erhebung, administrative Lizenzierung, Überwachung und Inspektion, administrative Sanktionen und andere Verwaltungsarbeiten in Bezug auf humangenetische Ressourcen zuständig.

Ausländische Organisationen, Einzelpersonen und die von ihnen gegründeten oder tatsächlich kontrollierten Einrichtungen dürfen weder chinesische humangenetische Ressourcen auf dem Gebiet Chinas sammeln und aufbewahren, noch dürfen sie chinesische humangenetische Ressourcen ins Ausland liefern.[43] Chinesische und ausländische Einrichtungen müssen gemeinsam beim China National Center for Biotechnology Development, einer vom NHC geleiteten Einrichtung, eine administrative Genehmigung für die internationale wissenschaftliche Zusammenarbeit und die Anmeldung von klinischen Studien für die internationale Zusammenarbeit beantragen.[44] Für die internationale Zusammenarbeit in der wissenschaftlichen Forschung unter Nutzung der humangenetischen Ressourcen Chinas müssen die chinesischen Einrichtungen und ihre Forschenden während des Zeitraums der Zusammenarbeit wesentlich am gesamten Forschungsprozess

DEFINITION
Zu den humangenetischen Ressourcen im Sinne der HGR-Vorschriften gehören sowohl Materialien als auch Informationen aus humangenetischen Ressourcen. Unter **Material aus humangenetischen Ressourcen** versteht man genetisches Material wie Organe, Gewebe und Zellen, die Erbsubstanzen wie menschliche Genome und Gene enthalten. **Informationen über humangenetische Ressourcen** beziehen sich auf Informationsmaterialien wie Daten, die aus Materialien über humangenetische Ressourcen gewonnen werden.

43 Artikel 7 HGR-Vorschriften.
44 Artikel 21 und 22 HGR-Vorschriften.

beteiligt sein, und alle Aufzeichnungen und Dateninformationen im Forschungsprozess müssen den chinesischen Einrichtungen zur Verfügung stehen, wobei den chinesischen Einrichtungen Sicherheitskopien zur Verfügung gestellt werden.[45] Um die Informationen über humangenetische Ressourcen dem Ausland zur Verfügung zu stellen oder zugänglich zu machen, muss der chinesische Eigentümer der Informationen dies im Voraus dem China National Center for Biotechnology Development melden und eine Sicherheitskopie der Informationen vorlegen.[46]

3.8.2 Verwaltungsmaßnahmen für die Datensicherheit im Bereich der natürlichen Ressourcen (NRDS-Maßnahmen)

Die NRDS-Maßnahmen wurden vom Ministerium für natürliche Ressourcen (**MNR**) am 22. März 2024 erlassen.

In Anbetracht der Merkmale von Daten im Bereich der natürlichen Ressourcen sind Daten, die mehr als zwei oder mehr der folgenden Referenzindikatoren erfüllen, im Kontext der natürlichen Ressourcen **wichtige Daten**:

(i) Unersetzliche und branchenweit einzigartige Daten, die zur Unterstützung staatlicher Aufgaben generiert werden, die sich auf die Aufgabenerfüllung von Behörden für natürliche Ressourcen auswirken und die eine wichtige Auswirkung auf landesweite Dienstleistungsobjekte haben, sobald ein Sicherheitsvorfall wie Datenmanipulation, Leckagen oder Dienstunterbrechungen eintritt (z. B. Wasserstände in Stauseen);

(ii) Daten, die sich auf die nationale Wirtschaft und den Lebensunterhalt von Menschen beziehen (z. B. Ernteerträge), die Unterstützung mit grundlegenden Daten über natürliche Ressourcen in anderen Industrien und Bereichen bieten und im Falle eines Datensicherheitsunfalls wichtige Auswirkungen auf andere Industrien und Bereiche haben;

(iii) Daten von großem Umfang, hoher Präzision, hoher Empfindlichkeit und Bedeutung, die mehrere Provinzen oder sogar das ganze Land abdecken;

(iv) Daten, die sich direkt auf den normalen Betrieb und die Dienstleistungen der nationalen CII auswirken (z. B. Telekommunikations- und Energieunternehmen);

(v) Daten, die die nationale Sicherheit und die nationale wirtschaftliche Wettbewerbsfähigkeit, den Zugang der Öffentlichkeit zu öffentlichen Diensten (z. B. städtische Verkehrsmittel, Versorgungseinrichtungen), die Lebensbedingungen der Bürgerinnen und Bürger und ein stabiles Arbeits- und Lebensumfeld, die Sicherheit von Leben und Eigentum der Bürgerinnen und Bürger und andere berechtigte Interessen gefährden oder zu sozialer Panik führen, usw. (z. B. Daten über Unruhen);

(vi) alle anderen wichtigen Daten über natürliche Ressourcen, die in den Gesetzen, Verordnungen und normativen Dokumenten Chinas vorgeschrieben sind.[47]

Wichtige Daten, die von einem Datenverarbeiter auf dem Gebiet Chinas erhoben und erstellt werden, müssen in China gespeichert werden.

45 Artikel 24 HGR-Vorschriften.

46 Artikel 28 HGR-Vorschriften.

47 Artikel 10 NDRS-Maßnahmen.

DEFINITION

Daten im Bereich der natürlichen Ressourcen sind definiert als Daten, die bei der Durchführung von Aktivitäten im Bereich der natürlichen Ressourcen gesammelt und generiert werden. Dazu gehören vor allem grundlegende geografische Informationen, Fernerkundungsbilder und andere geografische Informationen und Daten, Erhebungs- und Überwachungsdaten in Bezug auf natürliche Ressourcen wie Land, Mineralien, Wälder, Grünland, Wasser, Feuchtgebiete und Seegebiete sowie Inseln, Daten für die Raumplanung wie die Gesamtplanung, die Detailplanung und die Sonderplanung und Daten für die Verwaltung natürlicher Ressourcen wie die Nutzungskontrolle, die Vermögensverwaltung, der Schutz von Ackerland, die ökologische Wiederherstellung, die Entwicklung und Nutzung sowie die Registrierung von Immobilien.[48]

Praktische Bedeutung für Einrichtungen in Deutschland

Einrichtungen in Deutschland sollten aufmerksam sein, wenn Daten aus dem Bereich der natürlichen Ressourcen in Kooperationsprojekte einbezogen werden, insbesondere wenn diese Daten der oben genannten zusätzlichen Definition von wichtigen Daten entsprechen. Dies könnte z. B. im Falle eines Forschungsprojekts über die Auswirkungen des Wassermangels auf die landwirtschaftliche Produktion relevant sein. Die Sensibilität kann auch durch den betroffenen Standort (z. B. ein bestimmtes Meeresgebiet, eine Provinz, eine Insel), die Art des Bildes (z. B. ein Satellitenbild), einen Bezug zu Mineralien, Land- und Forstwirtschaft usw. angezeigt werden. Die Transparenzklausel ist hier mit dem Kooperationspartner zu vereinbaren, um die Rechte und Pflichten der Parteien diesbezüglich zu klären.

3.8.3 Bestimmungen für die Verwaltung der Netzwerkdatensicherheit (NDSM-Bestimmungen)

Die NDSM-Bestimmungen wurden vom Staatsrat erlassen und sind seit dem 1. Januar 2025 in Kraft.

Die NDSM-Bestimmungen haben einige offene Fragen bei der Umsetzung von CSL, DSL und PIPL geklärt. Sie zielen darauf ab, den Schutz von personenbezogenen Informationen und wichtigen Daten zu stärken. Der Anwendungsbereich der Netzwerkdaten-Verordnung ist weitreichend und erstreckt sich auch auf **alle digitalen Daten, die zwischen wissenschaftlichen Einrichtungen geteilt oder ausgetauscht werden.** Sie gelten für die chinesischen Kooperationspartner wie Universitäten oder wissenschaftliche Einrichtungen, die ein Netzwerk in China besitzen und/oder betreiben.

Die NDSM-Bestimmungen besagen, dass für Daten, die nicht von der jeweiligen Region oder anderweitig öffentlich als wichtige Daten bekannt gegeben wurden, **keine Sicherheitsbewertung für die grenzüberschreitende Übermittlung solcher Daten erforderlich ist.**

DEFINITION

Unter **Netzwerkdaten** versteht man verschiedene elektronische Daten, die über Netzwerke, wie z. B. ein lokales Netzwerk (LAN), verarbeitet und erzeugt werden.

48 Artikel 3 NRDS-Maßnahmen.

3.8.4 Nationale Norm GB/T 46068-2025 „Datensicherheitstechnologie – Sicherheitszertifizierungsanforderungen für grenzüberschreitende Verarbeitungsaktivitäten personenbezogener Daten“

Diese nationale Norm wurde am 29. August 2025 verkündet und tritt am 1. März 2026 in Kraft. Ihr Hauptinhalt umreißt grundlegende Prinzipien, Anforderungen und Schutzmaßnahmen für die Rechte der betroffenen Personen, wenn die an der Sicherheitszertifizierung beteiligten Parteien grenzüberschreitende Übermittlungen personenbezogener Daten aus China in ausländische Rechtsordnungen einrichten. Zu den Kernbestimmungen gehören: die Definition der zu zertifizierenden Stellen (inländische Verarbeiter personenbezogener Daten und Empfänger im Ausland); die Festlegung grundlegender Verpflichtungen wie den Abschluss rechtsverbindlicher Vereinbarungen und die Durchführung von Datenschutz-Folgenabschätzungen; die Wahrung individueller Rechte einschließlich des Rechts auf Information, Einwilligung, Widerruf der Einwilligung, Beschwerde und Wiedergutmachung; und die Verpflichtung zur laufenden Überwachung, wobei die Zertifizierungsstellen regelmäßige Überwachungsaudits durchführen, um die nachhaltige Einhaltung der grenzüberschreitenden Verarbeitungsaktivitäten sicherzustellen. Die nationale Norm verdeutlicht anhand von Anhängen typische Szenarien der grenzüberschreitenden Verarbeitung personenbezogener Daten und legt detaillierte Anforderungen an den Inhalt der Bewertung und die Risikoanalyse anhand einer Vorlage für Berichte zur Folgenabschätzung zum Schutz personenbezogener Daten fest. Die am 14. Oktober 2025 verkündeten und am 1. Januar 2026 in Kraft getretenen Maßnahmen zur Zertifizierung der grenzüberschreitenden Übermittlung personenbezogener Daten legen das Zertifizierungsverfahren für die grenzüberschreitende Übermittlung personenbezogener Daten und die Meldepflichten für professionelle Zertifizierungsstellen fest. Zusammen werden die oben genannte nationale Norm und die Maßnahmen die verfahrensrechtlichen und materiellen Verpflichtungen für die grenzüberschreitende Zertifizierung personenbezogener Daten präzisieren.

Praktische Bedeutung für Einrichtungen in Deutschland

Die in dieser nationalen Norm festgelegten Pflichten und Verantwortlichkeiten gelten nicht nur für inländische Verarbeiter personenbezogener Daten, sondern verlangen auch von Empfängern im Ausland, dass sie übertragene personenbezogene Daten schützen und die Rechte der betroffenen Personen durch vertragliche Verpflichtungen oder Zusagen wahren. Sollte ein Verarbeiter personenbezogener Daten den Ansatz der grenzüberschreitenden Zertifizierung wählen, verlangen die zuständigen Behörden oder professionellen Zertifizierungsstellen von Drittanbietern sowohl vom inländischen Verarbeiter als auch vom Empfänger im Ausland, dass sie die Bestimmungen dieser nationalen Norm gemäß ihren Anforderungen umsetzen. Im Rahmen dieses Zertifizierungsmodells müssen ausländische Einrichtungen in Deutschland erhöhte Compliance-Verpflichtungen gemäß den oben genannten nationalen Standards erfüllen.

4

Praktische Hinweise und Empfehlungen für deutsche Hochschulen

4.1 Forschungskooperationen mit China

Das KIWi empfiehlt – gemäß einer interessenorientierten, risikoreflexiven und kompetenzbasierten Ausgestaltung von Kooperationen mit China – jedes China-Projekt systematisch anzugehen, indem die mitgelieferte Checkliste (siehe Anlage) abgearbeitet wird. Dazu ist es erforderlich, sich ausreichende Hintergrundinformationen zu beschaffen. **Die folgenden Schlüsselfragen sollten immer gestellt werden**:

(1) Sind (sensible) personenbezogenen Informationen involviert (siehe **3.1**)?
(2) Sind wichtige Daten involviert (siehe **3.5**)?
(3) Ist ein CII-Betreiber involviert (siehe **3.4**)?
(4) Sind wissenschaftliche Daten involviert (siehe **3.3**)?
(5) Erfolgt ein Datentransfer von China ins Ausland (siehe **3.1** und **3.2**)?
(6) Sind kontrollierte Güter oder Güter mit doppeltem Verwendungszweck involviert (siehe **3.6**)?
(7) Sind humangenetische Ressourcen (siehe **3.8.1**) oder natürliche Ressourcen involviert (siehe **3.8.2**)?

Wenn die Antwort auf eine oder mehrere der Fragen ja lautet, muss der chinesische Kooperationspartner die notwendigen gesetzlichen Verpflichtungen, Genehmigungen oder Anmeldungen gemäß CSL, PIPL sowie anderen damit zusammenhängenden Gesetzen und Vorschriften durchlaufen und **abschließen, während die Einrichtung in Deutschland die notwendige Unterstützung und Zusammenarbeit in dem von den Gesetzen und Vorschriften vorgeschriebenen Umfang leisten sollte**. Alle entsprechenden vertraglichen Verpflichtungen und die Trennung/Teilung von Verbindlichkeiten für die Kooperationspartner können in einem schriftlichen Kooperationsrahmenvertrag und weiteren Vereinbarungen festgelegt werden.

Um die Risiken zu verringern, die Einhaltung der Vorschriften zu verbessern und die Beschaffung relevanter Informationen zu erleichtern, könnte **die folgende oder eine ähnliche Klausel zur Transparenz** in ein Memorandum of Understanding (MoU), eine Rahmenvereinbarung über die Zusammenarbeit und andere Vereinbarungen zwischen den Kooperationspartnern aufgenommen werden (die an den konkreten Einzelfall angepasst werden muss):

„Bevor eine Partei („**datenbekanntgebende Partei**“) Daten an die andere Partei weitergibt, informiert sie die andere Partei („**datenempfangende Partei**“) schriftlich über alle relevanten Compliance-Aspekte im Zusammenhang mit diesen Daten. Diese Informationspflicht umfasst Informationen über alle erforderlichen Voraussetzungen für eine Weitergabe (einschließlich z. B. erforderlicher Zustimmungen, Genehmigungen, Bewertungen, Zertifizierungen, Anmeldungen, technischer Maßnahmen, Abschluss von Standardverträgen). Die datenbekanntgebende Partei informiert die datenempfangende Partei außerdem unverzüglich über alle diesbezüglichen Anfragen von Regierungsbehörden und über alle relevanten Änderungen von Gesetzen oder Vorschriften im Zuständigkeitsbereich der datenbekanntgebenden Partei. Die datenempfangende Partei unterstützt die datenbekanntgebende Partei dabei, die Compliance-Aspekte vollständig einzuhalten.
[Der chinesische Kooperationspartner] stellt insbesondere die vollständige Einhaltung aller geltenden chinesischen Gesetze und Vorschriften sicher, einschließlich des Gesetzes zum Schutz personenbezogener Informationen, der Bestimmungen zur Förderung und Regulierung des grenzüberschreitenden Datenverkehrs, des Gesetzes zur Cybersicherheit, des Datenschutzgesetzes, der Maßnahmen zur Verwaltung von wissenschaftlichen Daten, des Ausfuhrkontrollgesetzes, des Gesetzes zur Spionageabwehr, des Gesetzes zur Wahrung von Staatsgeheimnissen, der Verwaltungsvorschriften über humangenetische Ressourcen, der Verwaltungsmaßnahmen für die Datensicherheit im Bereich der natürlichen Ressourcen, der Bestimmungen für die Verwaltung der Netzwerkdatensicherheit, der Verwaltungsvorschriften für den Import und Export von Technologie usw.
[Der deutsche Kooperationspartner] stellt insbesondere die vollständige Einhaltung aller geltenden deutschen und EU-Gesetze und -Vorschriften, einschließlich der Datenschutz-Grundverordnung (DSGVO), sicher.“

4.2 Schutz der Rechte an geistigem Eigentum

Beispiele für wichtige Themen, die in der Kooperationsvereinbarung geregelt werden sollten:

(1) das alleinige oder gemeinsame Eigentum an den Forschungsergebnissen;
(2) das alleinige oder gemeinsame Recht, Patente, Marken und Urheberrechte anzumelden, sowie die damit verbundenen Unterhaltskosten;
(3) das alleinige oder gemeinsame Recht der Kooperationspartner, die Forschungsergebnisse zu nutzen, sowie alle eingetragenen Rechte an geistigem Eigentum;
(4) die Bedingungen für die Übertragung des geistigen Eigentumsrechts an einen Dritten;
(5) das alleinige oder gemeinsame Recht, das Forschungsergebnis zu veröffentlichen;
(6) das Recht auf vorherige Zustimmung unter bestimmen Umständen;
(7) die Verteilung von Einkünften aufgrund des Forschungsergebnisses;
(8) anwendbares Recht und Zuständigkeit.

4.3 Streitschlichtung

Die Schiedsgerichtsbarkeit ist der bevorzugte Mechanismus zur Streitbeilegung. In der Praxis ist es immer noch nicht möglich, eine Entscheidung/ein Urteil eines ordentlichen/staatlichen deutschen Gerichts gegen einen Beklagten in China zu vollstrecken, da es kein gegenseitiges Vollstreckungsabkommen gibt. Im Gegensatz dazu sind Schiedssprüche in beiden Ländern vollstreckbar.

Die Parteien können eine **internationale Schiedsinstitution** in China, z. B. die China International Economic and Trade Arbitration Commission (CIETAC), in Deutschland z. B. die Deutsche Institution für Schiedsgerichtsbarkeit (DIS) oder an einem neutralen Ort wie Singapur z. B. das Singapore Arbitration Centre (SIAC), einschalten.

Als materielles Recht kann **entweder chinesisches oder deutsches Recht** gewählt werden. Falls der chinesische Kooperationspartner auf **chinesischem Recht** besteht, kann dies ebenfalls akzeptiert werden, wenn der Vertrag **von einer Rechtsanwältin oder einem Rechtsanwalt mit ausreichender Erfahrung im chinesischen, deutschen und internationalen Rechtsumfeld sorgfältig geprüft wird**.

4.4 Stipendienprogramme, Studierendenaustausch, gemeinsame Promotionsprogramme einschließlich Online-Bewerbungsportale, gemeinsame Studienprogramme

Für diese Programme werden sensible, personenbezogene Daten chinesischer Studierender, beispielsweise Identitäts-, Finanz- oder Gesundheitsdaten von Einrichtungen in Deutschland gesammelt oder verarbeitet. In diesen Fällen ist das PIPL auf Einrichtungen in Deutschland[49] anwendbar, die Bildungsdienstleistungen für chinesische Studierende anbieten. Das PIPL erfordert theoretisch die Benennung einer Vertreterin oder eines Vertreters in China.[50] In der **Praxis** wird diese Vorschrift jedoch vom deutschen Verarbeiter personenbezogener Informationen oft nicht umgesetzt, da es an Aufsicht mangelt und keine spezifischen Sanktionen vorgesehen sind. Wenn eine chinesische Behörde einen Verstoß im Zusammenhang mit solchen Daten feststellt, wendet sie sich in der Regel an die Einrichtung in China, die die Daten ins Ausland weitergegeben hat.

In bestimmten Fällen muss es sich bei dem offiziellen Verarbeiter und Exporteur solcher personenbezogenen Informationen um eine vom Bildungsministerium (MOE) für die internationale Bildungskooperation zugelassene Einrichtung oder Organisation in China handeln. Dieser chinesischen Organisation (dem offiziellen Verarbeiter in China) sollten vertraglich die wichtigsten Verpflichtungen zur Einhaltung der Datenschutzbestimmungen auferlegt werden, z. B. in Bezug auf Informationspflichten, Einholung einer (widerruflichen) Zustimmung, Formulierung einer PIPIA usw. Die Einrichtungen in Deutschland können zur Unterstützung durch technische und verwaltungstechnische Maßnahmen beitragen, z. B. die umfassende Information der Personen, die Einholung einer (widerruflichen) allgemeinen Zustimmung und einer besonderen Zustimmung, die Veröffentlichung klarer und transparenter Regeln für die Verarbeitung personenbezogener Informationen internationaler Studierender usw.

49 Artikel 3 Abs. 2 PIPL sieht vor, dass das PIPL auf die Verarbeitung personenbezogener Informationen natürlicher Personen innerhalb und außerhalb Chinas Anwendung findet, wenn einer der folgenden Umstände vorliegt: (i) wenn der Zweck darin besteht, inländische natürliche Personen mit Produkten oder Dienstleistungen zu versorgen; (ii) wenn die Aktivitäten inländischer natürlicher Personen analysiert und bewertet werden und (iii) unter anderen Umständen, die durch Gesetze und Vorschriften vorgeschrieben sind.

50 Artikel 53 PIPL.

4.5 Prüfungsrelevanter Datenaustausch

Auf der Grundlage der CBDF-Bestimmungen ist die grenzüberschreitende Übermittlung personenbezogener Informationen für Prüfungsleistungen und für Visumanträge von der Sicherheitsprüfung durch die CAC, von der Zertifizierung oder dem Abschluss eines Standardvertrags ausgenommen. Der offizielle Verarbeiter der betroffenen personenbezogenen Informationen in China muss jedoch immer noch die entsprechenden Verpflichtungen gemäß des PIPL erfüllen, wie z. B. die Betroffenen über die Verwendungszwecke, die Verarbeitungsmethoden usw. informieren, die entsprechende (widerrufliche) Zustimmung der Betroffenen einholen und den PIPIA ausfüllen.

Beim Personalaustausch müssen auch die Compliance bei der grenzüberschreitenden Übermittlung personenbezogener Informationen sowie die Einwanderungsbestimmungen beachtet werden. Darüber hinaus sollte die Einrichtung in Deutschland bei der Aufnahme chinesischer Mitarbeiterinnen und Mitarbeiter in der Einrichtung in Deutschland ausreichende Anstrengungen unternehmen, um die Vertraulichkeit zu gewährleisten, und zwar sowohl durch technische Mittel wie z. B. Beschränkungen des IT-Zugangs als auch durch vertragliche Beschränkungen wie z. B. durchsetzbare Vertraulichkeitsvereinbarungen mit Schiedsklauseln.

4.6 Best Practice für den Schutz von Forschungsdaten

Einrichtungen in Deutschland mögen es vorziehen, chinesische Daten **auf Servern außerhalb Chinas** zu speichern oder zu sichern, oder sie können von Übersee aus online auf chinesische Daten zugreifen. Solange es sich dabei **nicht um wichtige Daten oder personenbezogene Informationen handelt**, ist dies **erlaubt**. In allen **anderen Fällen** löst dieser grenzüberschreitende Datenexport e**ine hohe rechtliche Komplexität aus.** Der konkrete Einzelfall muss dann sorgfältig geprüft werden, bevor er auf der Grundlage der skizzierten Regeln umgesetzt wird.

Beispiel: *Ein chinesisches Genforschungsunternehmen und ein großes chinesisches Krankenhaus führten zusammen mit einer namhaften britischen Universität internationale Forschungen über humangenetische Ressourcen ohne Erlaubnis durch. Das Unternehmen stellte bestimmte genetische Daten online zur Verfügung und verstieß damit gegen die HGR-Vorschriften. Es wurde angewiesen, die Forschung zu stoppen, nicht exportierte Materialien zu vernichten und die interne Zusammenarbeit im Bereich der genetischen Ressourcen einzustellen, bis die Vorschriften eingehalten werden.*[51] *Dies zeigt, wie wichtig es ist, die chinesischen Datenexportgesetze und -vorschriften einzuhalten, im aktuellen Fall insbesondere auch die HGR-Vorschriften und die erforderlichen Verfahren mit dem China National Center for Biotechnology Development. Die Kenntnis der einschlägigen Gesetze und Vorschriften und die frühzeitige Befragung der Einrichtung in China zur Einhaltung der Vorschriften hätten die entsprechenden Risiken erheblich verringern können.*

51 https://www.most.gov.cn/xxgk/xinxifenlei/fdzdgknr/xzcf/202302/t20230228_184773.html.

4.7 Lizenzvereinbarungen für den Import und Export von Technologie und Know-how

China **regelt den Import und Export von Technologie und Know-how durch eine Klassifizierung in verbotene, eingeschränkte und erlaubte Technologien.** Verbotene Technologien dürfen nicht transferiert werden, während für eingeschränkte Technologien eine Genehmigung der Regierung erforderlich ist. Zugelassene Technologien können frei transferiert werden, können aber von behördlichen Vertragshinterlegungspflichten tangiert sein.[52]

Exporteure müssen sich in sensiblen Bereichen wie KI oder Halbleiter zusätzlichen Prüfungen unterziehen, und alle Transfers unterliegen dem Schutz der nationalen Sicherheit und des geistigen Eigentums. **Für Einrichtungen in Deutschland bedeutet dies, dass eine sorgfältige Vorabprüfung erforderlich ist, um die Art der Technologie zu bestimmen, falls Forschungsergebnisse (Technologie oder Know-how), die in China geschaffen wurden, nach Deutschland exportiert werden sollen.**

4.8 Konflikte, wenn sowohl das PIPL als auch die DSGVO einen Standardvertrag verlangen

Der **Abschluss eines Standardvertrags** unter dem PIPL kann eine rechtliche Option sein, wenn personenbezogene Informationen von China nach Deutschland fließen sollen. Die „vorgeprüften" *Standardvertragsklauseln* (SCC) unter der DSGVO müssen umgekehrt in den meisten Fällen für den Fluss personenbezogener Informationen aus der EU nach China verwendet werden. Die Überschneidung von Rechten, Pflichten und Konfliktlösungen muss sorgfältig behandelt werden.

Mögliche Lösungsansätze: Falls machbar, segmentieren Sie die Datenströme. Daten, die der DSGVO unterliegen, sollten nur unter SCC fließen, und Daten, die dem PIPL unterliegen, fließen nur unter dem chinesischen Standardvertrag. Fügen Sie einen **PIPL-Zusatz zum SCC** hinzu, der spezifische zusätzliche Anforderungen auf der Grundlage des PIPL festlegt.

Was die Datensegmentierung betrifft, so muss zunächst bestimmt werden, welche Daten unter welches System fallen.

Beispiel: *Eine Einrichtung in China speichert wissenschaftliche Daten in einer Datenbank, die von einer Einrichtung in Deutschland gehostet wird. Dies stellt einen Datenexport von China nach Deutschland dar. Daten, die dem PIPL unterliegen, sollten nur unter einem staatlich formulierten chinesischen Standardvertrag fließen.*

52 *Verwaltungsvorschriften für den Import und Export von Technologie* (2020).

4.9 Nutzung digitaler Tools für Backgroundchecks durch deutsche Hochschulen

Digitale Tools können für die Auswahl von akademischen Bewerberinnen und Bewerbern grundsätzlich auch von Einrichtungen in Deutschland genutzt werden, **ein solches Vorgehen erfordert jedoch eine sorgfältige Vorabprüfung**. Neben der **Einhaltung der DSGVO einschließlich z. B. der Schufa-Entscheidung**[53] **sollte** die Einrichtung in Deutschland in einem solchen Fall auch **die PIPL-Anforderungen berücksichtigen**. Wenn die digitalen Werkzeuge von Drittanbietern bereitgestellt werden, sollte die Einrichtung in Deutschland ebenfalls sicherstellen, dass diese Anbieter sowohl die DSGVO als auch das PIPL einhalten, z. B. durch entsprechende Vertragsklauseln, die die Anbieter verpflichten.

Sowohl DSGVO als auch PIPL verlangen Transparenz über den Zweck, die Logik und die Auswirkungen von automatisierten Prozessen. Die Einrichtung in Deutschland muss bei Nutzung des digitalen Tools **klar offenlegen, wie die Daten analysiert werden und wie Entscheidungen getroffen werden, damit die Bewerberinnen und Bewerber die Kriterien für ihre Auswahl verstehen**.

Nach beiden Gesetzen haben Bewerberinnen und Bewerber das **Recht, Entscheidungen anzufechten, ein menschliches Eingreifen zu verlangen und sich gegen eine ausschließlich automatisierte Bewertung zu entscheiden**, insbesondere wenn die Entscheidung ihre Rechte oder Interessen erheblich beeinträchtigt.

Die Einrichtungen müssen **für Fairness sorgen und Diskriminierung verhindern, indem sie verzerrte Eingabedaten oder** Kriterien vermeiden, die Kandidatinnen und Kandidaten aufgrund von Faktoren wie Nationalität oder sozioökonomischem Status benachteiligen könnten. Regelmäßige Prüfungen des Algorithmus sollten durchgeführt werden, um Verzerrungen aufzudecken, die Repräsentativität sicherzustellen und die Einhaltung der Vorschriften zu bestätigen. Zu den Maßnahmen der Rechenschaftspflicht gehören die **Dokumentation der Entwicklung, der Tests und der Implementierung des Systems sowie die Durchführung von z. B. einer PIPIA, um Risiken zu minimieren**. Um Streitigkeiten zu mitigieren, sollten Einrichtungen in Deutschland **menschliche Aufsicht** in wichtige Entscheidungen einbeziehen und klare Protokolle zur Erläuterung automatisierter Ergebnisse erstellen.

53 https://curia.europa.

4.10 Ausblick: Die Rolle von Treuhänder-Einrichtungen im deutschen und chinesischen Recht

Das geplante deutsche Forschungsdatengesetz sieht u.a. die Einrichtung von sogenannten „Mikrodatenzentren“ vor. Dabei handelt es sich um zentrale Datentreuhandstellen, die Forschenden einen sicheren und vereinfachten Zugang zu statistischen Daten und Registerdaten bieten sollen. Ziel ist es, die Nutzung öffentlicher Daten (ohne Entgelt) für wissenschaftliche Zwecke sowie die Auffindbarkeit von Forschungsdaten zu erleichtern und gleichzeitig einen soliden Datenschutz zu gewährleisten.

China fördert auch die Nutzung staatlicher und öffentlicher Daten und ermutigt qualifizierte Einrichtungen, den Betrieb solcher staatlicher und öffentlicher Daten zu genehmigen.[54] Lokale Volksregierungen auf oder oberhalb der Kreisebene und die zuständigen staatlichen Industrieabteilungen können öffentliche Datenressourcen, die sich im Einklang mit dem Gesetz befinden, für den autorisierten Betrieb durch qualifizierte Einrichtungen zur Verfügung stellen. Diese Einrichtungen registrieren die öffentlichen Datenressourcen, öffentliche Datenprodukte und -dienste im Rahmen des autorisierten Betriebs gemäß den Anforderungen für die Registrierung und Verwaltung öffentlicher Datenressourcen.[55] Die Preise für öffentliche Datenprodukte und -dienste richten sich nach der jeweiligen nationalen Preispolitik.

Die autorisierte Betreiberorganisation muss die interne Verwaltung von Kosten, Einnahmen und Ausgaben im Zusammenhang mit öffentlichen Datenprodukten und -diensten stärken und die finanziellen Einnahmen und Ausgaben im Zusammenhang mit öffentlichen Datenprodukten und -diensten in Übereinstimmung mit dem bestehenden Finanzmanagementsystem verwalten. **Der Zweck des oben genannten genehmigten Betriebs öffentlicher Datenressourcen konzentriert sich auf die kommerzielle Nutzung** von Daten und unterscheidet sich von dem der „Mikrodatenzentren“ nach dem geplanten deutschen Gesetz.

Im Rahmen der ASD-Maßnahmen können die zuständigen Ministerien qualifizierte Einrichtungen zur Implementierung von „wissenschaftlichen Datenzentren“ ermächtigen. Der Zweck dieser Zentren ist es, wissenschaftliche Daten zu sammeln und zu speichern, die mit Unterstützung der Regierung erstellt wurden. Unter verschiedenen Voraussetzungen können die Daten mit der Öffentlichkeit und den zuständigen Behörden geteilt werden, um **den Kanal für den Austausch wissenschaftlicher Daten zwischen dem militärischen und dem zivilen Sektor freizugeben.** Auch dies ist ein Unterschied zu den „Mikrodatenzentren“ im Rahmen des geplanten deutschen Gesetzes.

54 *Stellungnahmen des Generalbüros des Staatsrats zur Beschleunigung der Entwicklung und Nutzung öffentlicher Datenquellen* (2024).

55 *Spezifikation für die Implementierung des autorisierten Betriebs von öffentlichen Datenressourcen (Versuch)* (2024).

5

Zusammenfassung

Internationale Wissenschaftskooperationen bringen große Potenziale für Forschung und Innovation mit sich, die nur auf der Grundlage einer vertrauensvollen Zusammenarbeit und in einem geregelten Rahmen entfaltet werden können. Dazu gehört auch, die Rechte und Pflichten der Kooperationspartner auf vertraglicher Grundlage zu definieren und die jeweils auf nationaler oder regionaler Ebene geltenden gesetzlichen Bestimmungen zu kennen und in der Vertragsgestaltung mit einzubeziehen. In internationalen Wissenschaftskooperationen ist das Thema Datenschutz ein unverzichtbarer Gegenstand der Vertragsgestaltung und der entsprechenden Aushandlungsprozesse zwischen den Partnern.

Der vorliegende KIWi Kompass „Datenschutz in China“ widmet sich der datenschutzrechtlichen Dimension der wissenschaftlichen Zusammenarbeit mit China und reagiert damit auf Unterstützungsbedarfe deutscher Hochschulen, die sich in der Beratungspraxis des KIWi besonders häufig äußern. Im Fokus stehen hier die chinesischen Datenschutzvorgaben. Es ist jedoch ausdrücklich zu betonen, dass in der Kooperation auch und gerade mit China – die deutschen und europäischen Datenschutzvorgaben uneingeschränkt gelten und im Kooperationskontext vorrangig zu beachten sind.

Zentrale Gesetze sind insbesondere das Gesetz zum Schutz personenbezogener Informationen (PIPL), das Datensicherheitsgesetz (DSL), das Cybersicherheitsgesetz (CSL) sowie ergänzende Regelwerke wie die Bestimmungen zur Förderung des grenzüberschreitenden Datenverkehrs (CBDF-Bestimmungen), die Maßnahmen für wissenschaftliche Daten (ASD-Maßnahmen) und das Ausfuhrkontrollgesetz (ECL). Diese Normen regeln die Verarbeitung personenbezogener Daten, die Kategorisierung und den Export wichtiger Daten, die Sicherheit kritischer Infrastrukturen sowie die Übermittlung von Daten ins Ausland. Sie unterliegen regelmäßigen Anpassungen und stellen hohe Anforderungen an Transparenz, Zustimmungspflichten und Compliance.

Die rechtlichen Verpflichtungen durch chinesische Gesetze und Vorgaben liegen in den meisten Fällen bei den chinesischen Partnerinstitutionen. Gleichwohl können auch deutsche Hochschulen und Forschende indirekt betroffen sein, wie etwa durch die Aussetzung von Datentransfers, wenn ein chinesischer Partner

gegen Vorgaben verstößt, oder durch verwaltungsrechtliche Risiken im Fall grober Missachtung chinesischer Bestimmungen. Besondere Aufmerksamkeit erfordern Kooperationen mit gemeinschaftlich betriebenen deutsch-chinesischen Einrichtungen in China oder bei längeren Forschungsaufenthalten deutscher Wissenschaftlerinnen und Wissenschaftlern vor Ort, da hier die chinesischen Regelungen unmittelbar greifen.

Grundsätzlich wird im Einklang mit dem DAAD-Perspektivenpapier „Die akademische Zusammenarbeit mit China realistisch gestalten“ auch in diesem KIWi Kompass die Prämisse zugrunde gelegt, Kooperationen mit China interessenorientiert, risikoreflexiv und kompetenzbasiert auszurichten. Im Zusammenhang mit den rechtlichen Rahmenbedingungen einer Kooperation bedeutet dies, Chancen und Risiken systematisch abzuwägen, rechtliche Rahmenbedingungen frühzeitig zu klären und klare vertragliche Regelungen zu treffen. Hilfreich sind etwa Transparenzklauseln zu rechtlichen Änderungen, Vereinbarungen zur Trennung von Verantwortlichkeiten sowie Musterformulierungen. Hierzu liefert der vorliegende Leitfaden praktische Beispiele, die für die Kooperationsgestaltung der Hochschulen zugrunde gelegt bzw. an die spezifischen Rahmenbedingungen des betreffenden Kooperationsvorhabens angepasst werden können. Einrichtungen in Deutschland sollten zudem proaktiv mit ihren chinesischen Partnern und Behörden interagieren, indem sie etwaige Bedenken offen, möglichst schriftlich und im Voraus adressieren. Darüber hinaus sollten Fragen des Schutzes geistigen Eigentums, der Streitbeilegung (z. B. Schiedsgerichtsbarkeit) und der gegenseitigen Informationspflichten in die Vertragsgestaltung aufgenommen werden. Eine Checkliste in der Anlage unterstützt Einrichtungen dabei, relevante Fragestellungen, von der Einbindung sensibler personenbezogener Daten bis zur Beteiligung kritischer Infrastrukturen, systematisch zu prüfen.

Die chinesischen Datenschutzgesetze sind streng und unterliegen regelmäßigen Anpassungen. Aus diesem Grund ist es wichtig, auf Aktualisierungen zu achten und regelmäßig in den Austausch zu gehen. Der DAAD bietet hierfür mit dem KIWi fundierte Informations- und Beratungsangebote für internationale Wissenschaftskooperationen und verbindet dies mit der regionalen Expertise aus dem weltweiten DAAD-Netzwerk. Durch Einbindung des Außennetzwerks mit Kolleginnen und Kollegen vor Ort in China und den Erfahrungsaustausch mit deutschen Hochschulen können Herausforderungen und passende Lösungen gefunden und geteilt werden. **In sensiblen oder risikobehafteten Forschungsprojekten ist eine weiterführende Rechtsberatung zu empfehlen, welche nicht durch das KIWi gewährleistet werden kann**.

Wichtigste Abkürzungen und Gesetze

ASD	**Administration of Scientific Data** | Verwaltung von wissenschaftlichen Daten **Wissenschaftliche Daten** werden definiert als Daten, die aus der Grundlagenforschung, der Anwendungsforschung, der Pilotentwicklung und anderen Bereichen wie Naturwissenschaften und Ingenieurwissenschaften stammen, sowie als Originaldaten und abgeleitete Daten, die durch Beobachtung und Überwachung, Erhebung und Untersuchung sowie Inspektion und Detektion gewonnen und für wissenschaftliche Forschungsaktivitäten verwendet werden. Chinesischer Text der Maßnahmen für die Verwaltung von wissenschaftlichen Daten Zuständige Behörde: MOST
CAC	**Cyberspace Administration of China** | Chinesische Cyberspace-Verwaltung
CBDF	**Cross-Border Data Flow** | Förderung und Regulierung des grenzüberschreitenden Datenverkehrs Chinesischer Text der Bestimmungen zur Förderung und Regulierung des grenzüberschreitenden Datenverkehrs Zuständige Behörde: CAC
CEL	**Counter-Espionage Law** | Gesetz zur Spionageabwehr **Spionage** ist definiert als: (i) Aktivitäten, die die nationale Sicherheit Chinas gefährden, begangen von einer Spionageorganisation, ihrer Agentin oder ihrem Agenten oder einer anderen Person, die von einer solchen Organisation oder einer solchen Agentin oder einem solchen Agenten angestiftet/finanziert wird/mit ihr/ihm konspiriert (zusammen: Spionin oder Spion); (ii) Beitritt zu einer Spionageorganisation oder Annahme eines Auftrags, der von einer Spionageorganisation oder ihrer Agentin oder ihrem Agenten erteilt wurde, oder Überlaufen zu einer Spionageorganisation oder ihrer Agentin oder ihrem Agenten; (iii) Diebstahl, Spionage, Kauf oder illegale Weitergabe von Staatsgeheimnissen, nachrichtendienstlichen oder anderen Dokumenten, Daten, Materialien oder Artikeln, die sich auf die nationale Sicherheit oder nationale Interessen beziehen, oder Anstiftung, Verlockung, Nötigung oder Bestechung einer Mitarbeiterin oder eines Mitarbeiters des Staates zum Überlaufen; (iv) Cyberangriffe, Eindringen, Beeinflussung, Kontrolle oder Zerstörung gegen ein staatliches Organ, eine geheimhaltungsrelevante Einrichtung oder eine CII usw., die von einer Spionin oder einem Spion begangen werden; (v) Anzeige von Angriffszielen für Feinde; und (vi) andere Spionageaktivitäten. Chinesischer Text des Spionageabwehrgesetzes Zuständige Behörden: MSS, PSB
CIETAC	**China International Economic and Trade Arbitration Commission** | Chinesische Internationale Wirtschafts- und Handelsschiedsgerichtskommission
CII	**Critical Information Infrastructures** | Kritische Informationsinfrastrukturen

CSL	**Cyber Security Law** | Cyber-Sicherheitsgesetz **Personenbezogene Informationen** sind definiert als verschiedene Informationen, die in elektronischer oder anderer Form aufgezeichnet und allein oder in Kombination mit anderen Informationen verwendet werden, um die Identität einer natürlichen Person zu erkennen, einschließlich Namen, Geburtsdatum, ID-Nummer, personenbezogene biometrische Daten, Adresse und Telefonnummer der natürlichen Person. **Kritische Informationsinfrastrukturen** (CII) werden definiert als Informationsinfrastrukturen in wichtigen Branchen und Sektoren wie öffentliche Kommunikation, Informationsdienste, Energie, Verkehr, Wasserwirtschaft, Finanzen, öffentlicher Dienst und elektronische Behördendienste sowie andere kritische Informationsinfrastrukturen, die im Falle einer Beschädigung, Deaktivierung oder Offenlegung von Daten die nationale Sicherheit, die Volkswirtschaft, den Lebensunterhalt der Menschen und die öffentlichen Interessen ernsthaft gefährden können. Chinesischer Text des Cybersicherheitsgesetzes Zuständige Behörden: CAC, PSB
DIS	**Deutsche Institution für Schiedsgerichtsbarkeit**
DSGVO	**Datenschutzgrundverordnung**
DSL	**Data Security Law** | Gesetz zur Datensicherheit **Personenbezogene Informationen** sind definiert als verschiedene Informationen, die in elektronischer oder anderer Form aufgezeichnet und allein oder in Kombination mit anderen Informationen verwendet werden, um die Identität einer natürlichen Person zu erkennen, einschließlich Namen, Geburtsdatum, ID-Nummer, personenbezogene biometrische Daten, Adresse und Telefonnummer der natürlichen Person. **Wichtige Daten** werden in den DSL- und NDSM-Bestimmungen als Daten in einem bestimmten Bereich, einer bestimmten Gruppe oder Region oder mit einer bestimmten Genauigkeit und einem bestimmten Umfang definiert, die, wenn sie manipuliert, zerstört, weitergegeben, unrechtmäßig erlangt oder unrechtmäßig verwendet werden, die nationale Sicherheit, den wirtschaftlichen Betrieb, die soziale Stabilität, die öffentliche Gesundheit und die Sicherheit direkt gefährden können. Weitere Details zu wichtigen Daten sollen für verschiedene Regionen und Abteilungen, Branchen usw. festgelegt werden. Die NDSM-Bestimmungen besagen jedoch, dass für Daten, die nicht von der jeweiligen Region oder Abteilung oder anderweitig öffentlich als wichtige Daten bekannt gegeben wurden, keine Sicherheitsbewertung für die grenzüberschreitende Übermittlung solcher Daten erforderlich ist. Die Pilot-Freihandelszonen sind ermächtigt, ihre eigenen Listen für wichtige Daten oder allgemeine Daten zu definieren. Bislang haben die Pilot-Freihandelszonen in Tianjin, Peking und Shanghai (einschließlich Lingang) entsprechende Negativlisten für wichtige Daten herausgegeben, während die Pilot-Freihandelszone in Shanghai Lingang eine Positivliste für drei Branchen veröffentlicht hat. Chinesischer Text des Datensicherheitsgesetzes Zuständige Behörden: CAC, Ministerien
ECL	**Export Control Law** | Ausfuhrkontrollgesetz **Als kontrollierte Güter** gelten z. B. militärische Produkte, nukleare und andere Güter, Technologien, Dienstleistungen und Gegenstände, die sich auf die Wahrung der nationalen Sicherheit beziehen. Dazu gehören auch technische Informationen und Daten im Zusammenhang mit diesen Gütern. **Güter mit doppeltem Verwendungszweck** sind definiert als Güter, Technologien und Dienstleistungen, die sowohl für zivile als auch für militärische Zwecke verwendet werden können oder die dazu geeignet sind, das militärische Potenzial zu erhöhen, insbesondere solche, die für die Entwicklung, Herstellung oder den Einsatz von Massenvernichtungswaffen und deren Trägermitteln verwendet werden können. Chinesischer Text des Exportkontrollgesetzes Zuständige Behörde: MOFCOM

HGR	**Human Genetic Resources** | Humangenetische Ressourcen **Zu den humangenetischen Ressourcen** gehören sowohl Materialien der humangenetischen Ressourcen als auch Informationen über humangenetische Ressourcen. **Unter Material aus humangenetischen Ressourcen** versteht man genetisches Material wie Organe, Gewebe und Zellen, die Erbsubstanzen wie menschliche Genome und Gene enthalten. **Informationen über humangenetische Ressourcen** sind definiert als Informationsmaterial wie z. B. Daten, die aus Material über humangenetische Ressourcen gewonnen wurden. Chinesischer Text der Verwaltungsvorschriften über humangenetische Ressourcen Zuständige Behörde: NHC
MLPS	**Multi-level protection system** | Mehrstufiges Schutzsystem
MNR	**Ministry of Natural Resources of China** | Chinesisches Ministerium für Natürliche Ressourcen
MOE	**Ministry of Education of China** | Chinesisches Bildungsministerium
MOFCOM	**Ministry of Commerce of China** | Chinesisches Handelsministerium
MOST	**Ministry of Science and Technology of China** | Chinesisches Ministerium für Wissenschaft und Technologie
SSL	**Law on Guarding State Secrets** | Gesetz zur Wahrung von Staatsgeheimnissen **Ein Staatsgeheimnis** ist definiert als eine Angelegenheit, die für die nationale Sicherheit und die nationalen Interessen von entscheidender Bedeutung ist und die gemäß den gesetzlichen Bestimmungen nur einem begrenzten Personenkreis für einen bestimmten Zeitraum zugänglich gemacht wird. Zu den Staatsgeheimnissen gehören Verschlusssachen aus Wissenschaft und Technik, die die nationale Sicherheit und die nationalen Interessen betreffen und deren Bekanntwerden die nationale Sicherheit und die Interessen in den Bereichen Politik, Wirtschaft, Landesverteidigung, Außenpolitik usw. gefährden kann. Chinesischer Text des Gesetzes zur Wahrung von Staatsgeheimnissen Zuständige Behörde: MSS
MSS	**Ministry of State Security of China** | Chinesisches Ministerium für Staatssicherheit
NDSM	**Network Data Security Management** | Verwaltung der Sicherheit von Netzwerkdaten **Unter Netzwerkdaten** versteht man verschiedene elektronische Daten, die über Netzwerke, wie z. B. ein lokales Netzwerk (LAN), verarbeitet und erzeugt werden. Chinesischer Text der Vorschriften zur Verwaltung der Sicherheit von Netzwerkdaten Zuständige Behörde: CAC
NHC	**National Health Commission** | Nationale Gesundheitskommission

NRDS	**Natural Resources Data Security** | Datensicherheit im Bereich der natürlichen Ressourcen **Daten im Bereich der natürlichen Ressourcen** sind definiert als Daten, die bei der Durchführung von Aktivitäten im Bereich der natürlichen Ressourcen gesammelt und generiert werden. Dazu gehören vor allem grundlegende geografische Informationen, Fernerkundungsbilder und andere geografische Informationen und Daten, Erhebungs- und Überwachungsdaten in Bezug auf natürliche Ressourcen wie Land, Mineralien, Wälder, Grünland, Wasser, Feuchtgebiete und Meeresgebiete und Inseln, Daten für die Raumplanung wie die Gesamtplanung, die Detailplanung und die Sonderplanung sowie Daten für die Verwaltung natürlicher Ressourcen wie die Nutzungskontrolle, die Vermögensverwaltung, der Schutz von Ackerland, die ökologische Wiederherstellung, die Entwicklung und Nutzung sowie die Registrierung von Immobilien. Chinesischer Text der Verwaltungsmaßnahmen für Datensicherheit im Bereich der natürlichen Ressourcen Zuständige Behörde: MNR
PIPIA	**Personal Information Protection Impact Assessment** | Datenschutz-Folgenabschätzung für personenbezogene Daten
PIPL	**Personal Information Protection Law** | Gesetz zum Schutz personenbezogener Informationen **Sensible personenbezogene Informationen** sind definiert als personenbezogene Informationen, die die persönliche Würde einer natürlichen Person verletzen oder ihre persönliche oder materielle Sicherheit beeinträchtigen können, wenn sie offengelegt oder unrechtmäßig verwendet werden. Dazu gehören Informationen wie biometrische Identifikation, religiöser Glaube, spezifische Identität, medizinischer Gesundheitszustand, Finanzkonto und Aufenthaltsort und Spuren sowie die personenbezogenen Informationen von Minderjährigen unter 14 Jahren. Chinesischer Text des Gesetzes zum Schutz personenbezogener Informationen Zuständige Behörden sind: CAC, PSB
PSB	**Public Security Bureaus** | Behörden für Öffentliche Sicherheit
SCC	**Standard Contract Clauses** | Standardvertragsklauseln
SIAC	**Singapore Arbitration Centre** | Schiedsgericht Singapur

Checkliste

zu chinesischen Datenschutzregelungen in akademischen Kooperationen

In den meisten Fällen liegen die gesetzlichen Verpflichtungen in den einschlägigen chinesischen Gesetzen und Vorschriften bei der Einrichtung in China. Es kann jedoch sein, dass die Einrichtung in Deutschland die Einrichtung in China proaktiv auffordern möchte, die Einhaltung der Vorschriften zu erreichen, und dass sie dabei unterstützen muss.

Im Folgenden findet sich eine Checkliste, die in acht thematische Blöcke gegliedert ist und insgesamt 40 Einzelfragen umfasst. Die Bearbeitung dieser Checkliste erfolgt in chronologischer Reihenfolge. Jede Frage ist mit den Antwortoptionen „Ja“ oder „Nein“ versehen. Wird Ihnen – abhängig von Ihrer Antwort – angezeigt, dass Sie mit einer anderen Frage fortfahren können, können alle Fragen bis zu dieser Stelle übersprungen werden. Sofern sich eine Frage nicht eindeutig mit „Ja“ oder „Nein“ beantworten lässt oder Unsicherheiten bzw. weitere Abstimmungsbedarfe bestehen, steht Ihnen im jeweiligen Block ein Freitextfeld zur Verfügung, das für ergänzende Notizen genutzt werden kann.

Allgemeine Datenübermittlung

1 **Erhält die Einrichtung in Deutschland während einer akademischen Zusammenarbeit Daten von der Einrichtung in China, bei denen es sich weder um personenbezogene Informationen noch um wichtige Daten handelt?**

◯ Ja ◯ Nein

Wenn ja, *ist die Übermittlung dieser Daten von bestimmten gesetzlichen Anforderungen ausgenommen und Sie können mit* ▶ **8** *fortfahren.*

Freifeld für Notizen

Übermittlung personenbezogener Daten

2 Erhält die Einrichtung in Deutschland personenbezogene Informationen von der Einrichtung in China?

◯ Ja ◯ Nein

Wenn nein, *fahren Sie mit* ▶ **6** *fort*

2.1 Erfüllt die Einrichtung in China die notwendigen Informationspflichten in China?

◯ Ja ◯ Nein

2.2 Ist die Datenübermittlung für den Abschluss oder die Erfüllung eines Vertrags erforderlich, bei dem die betroffene Person Vertragspartei ist (z. B. Vertrag über Studiengebühren mit einer Einrichtung in Deutschland)?

◯ Ja ◯ Nein

Wenn ja, *ist keine Zustimmung der betroffenen Person erforderlich. Fahren Sie bitte mit* ▶ **2.6** *fort.*

2.3 Ist die Datenübermittlung für die Durchführung der Personalverwaltung erforderlich?

◯ Ja ◯ Nein

Wenn ja, *ist keine Zustimmung der Person erforderlich, fahren Sie bitte mit* ▶ **2.6** *fort.*

2.4 Falls eine Zustimmung erforderlich ist, holt die Einrichtung in China allgemeine und spezielle Zustimmungen in China ein?

◯ Ja ◯ Nein

2.5 Erstellt die Einrichtung in China eine notwendige Folgenabschätzung zum Schutz personenbezogener Informationen (PIPIA) in China und reicht sie diese bei der Behörde ein?

◯ Ja ◯ Nein

2.6 Werden im Zeitraum ab dem 1. Januar eines bestimmten Jahres personenbezogene Informationen (mit Ausnahme sensibler personenbezogener Informationen) von weniger als 100.000 Personen übermittelt?

◯ Ja ◯ Nein

Wenn ja, *fahren Sie mit* ▶ **3** *fort.*

2.7 Handelt es sich um personenbezogene Informationen, die ursprünglich im Ausland erhoben oder erstellt wurden und dann nach China übermittelt und dort verarbeitet werden, ohne dass vor der Wiederausfuhr in China erstellte personenbezogene Informationen oder wichtige Daten hinzugefügt werden?

◯ Ja ◯ Nein

Wenn ja, *fahren Sie mit* ▶ **3** *fort.*

2.8 Sind die personenbezogenen Informationen (einschließlich sensibler personenbezogener Informationen) erforderlich, um einen Vertrag für eine natürliche Person als Vertragspartner abzuschließen und zu erfüllen, z. B. für grenzüberschreitende Einkäufe, Lieferdienste, Überweisungen, Zahlungen, Kontoeröffnungen, Flugticket- und Hotelbuchungen, Visumanträge oder Prüfungsdienstleistungen?

◯ Ja ◯ Nein

Wenn ja, *fahren Sie mit* ▶ **3** *fort.*

2.9 Werden personenbezogene Informationen (einschließlich sensibler personenbezogener Informationen) interner Mitarbeiterinnen und Mitarbeiter zur Umsetzung der Personalverwaltung im Ausland in Übereinstimmung mit den formulierten arbeitsrechtlichen Vorschriften und den gemäß dem Gesetz unterzeichneten Tarifverträgen übermittelt?

◯ Ja ◯ Nein

Wenn ja, *fahren Sie mit* ▶ **3** *fort.*

2.10 Müssen die personenbezogenen Informationen (einschließlich sensibler personenbezogener Informationen) in einem Notfall übermittelt werden, um das Leben, die Gesundheit oder das Eigentum von natürlichen Personen zu schützen?

◯ Ja ◯ Nein

Wenn ja, *fahren Sie mit* ▶ **3** *fort.*

2.11 In anderen Fällen als den oben genannten 2.6 bis 2.10: Ist bei der Ausfuhr der personenbezogenen Informationen aus China eine der drei möglichen Bedingungen erfüllt:
(1) Sicherheitsbewertung durch die CAC, oder (2) Zertifizierung der Einrichtung in China, oder
(3) Abschluss eines Standardvertrags zwischen der Einrichtung in China und der Einrichtung in Deutschland?

◯ Ja ◯ Nein

2.12 Hat die Einrichtung in China für den Export personenbezogener Informationen aus China zusätzlich zu 2.4 die gesonderte Einwilligung in China eingeholt?

◯ Ja ◯ Nein

3 **Stellt ein Betreiber kritischer Informationsinfrastrukturen (CII) in China personenbezogene Informationen zusätzlich zu den unter 2.7 bis 2.10 ausgenommenen personenbezogenen Informationen an die Einrichtung in Deutschland zur Verfügung?**

◯ Ja ◯ Nein

Wenn ja, *führt der chinesische CII-Betreiber eine Sicherheitsbewertung durch die CAC durch?*

◯ Ja ◯ Nein

---

4 **Handelt es sich um einen Datenverarbeiter in China, bei dem es sich nicht um einen CII-Betreiber handelt, und der der Einrichtung in Deutschland seit dem 1. Januar eines bestimmten Jahres insgesamt die personenbezogenen Informationen (mit Ausnahme sensibler personenbezogener Informationen) von mehr als 100.000, aber weniger als 1 Million Personen zur Verfügung stellt, oder der der Einrichtung in Deutschland seit dem 1. Januar eines bestimmten Jahres insgesamt sensible personenbezogene Informationen von weniger als 10.000 Personen zur Verfügung stellt?**

◯ Ja ◯ Nein

Wenn ja, *ist der chinesische Datenverarbeiter von einer spezialisierten Agentur zertifiziert worden oder wurde ein Standardvertrag mit der Einrichtung in Deutschland abgeschlossen?*

◯ Ja ◯ Nein

---

5 **Liefert ein Datenverarbeiter in China, der kein CII-Betreiber ist, zum 1. Januar eines bestimmten Jahres personenbezogene Informationen (mit Ausnahme sensibler personenbezogener Informationen) von mehr als 1 Million Menschen oder sensible personenbezogene Informationen von mehr als 10.000 Menschen insgesamt an die Einrichtung in Deutschland?**

◯ Ja ◯ Nein

Wenn ja, *führt der chinesische Datenverarbeiter eine Sicherheitsbewertung durch die CAC durch?*

◯ Ja ◯ Nein

Freifeld für Notizen

Transfer wichtiger Daten

6 **Erhält die Einrichtung in Deutschland wichtige Daten von der Einrichtung in China?**

◯ Ja ◯ Nein

Wenn nein, *fahren Sie mit* ▶ **8** *fort.*
Wenn ja, *liefert ein anderer Datenverarbeiter in China als ein CII-Betreiber wichtige Daten an die Einrichtung in Deutschland?*

◯ Ja ◯ Nein

Wenn ja, *führt der chinesische Datenverarbeiter eine Sicherheitsüberprüfung durch die CAC durch?*

◯ Ja ◯ Nein

---

7 **Liefert ein CII-Betreiber in China wichtige Daten an die Einrichtung in Deutschland?**

◯ Ja ◯ Nein

Wenn ja, *führt der chinesische CII-Betreiber eine Sicherheitsüberprüfung durch die CAC durch?*

◯ Ja ◯ Nein

Freifeld für Notizen

Transfer wissenschaftlicher Daten

8 **Bekommt die Einrichtung in Deutschland wissenschaftliche Daten von der Einrichtung in China?**

◯ Ja ◯ Nein

Wenn nein, *fahren Sie mit* ▶ **9** *fort.*

8.1 Die vorrangige Verantwortung für wissenschaftliche Daten liegt in China bei wissenschaftlichen Forschungsinstituten, Universitäten, Unternehmen und anderen juristischen Personen sowie bei wissenschaftlichen Datenzentren. Ist die Einrichtung in China ihren gesetzlichen Verpflichtungen nachgekommen?

◯ Ja ◯ Nein

8.2 Wurden die wissenschaftlichen Daten im Rahmen eines wissenschaftlichen und technologischen Planungsprojekts gewonnen, das mit staatlichen Mitteln unterstützt wurde?

◯ Ja ◯ Nein

Wenn ja, *hat die Einrichtung in China die wissenschaftlichen Daten an das entsprechende wissenschaftliche Datenzentrum übermittelt?*

◯ Ja ◯ Nein

8.3 Wurde eine Arbeit auf der Grundlage wissenschaftlicher Daten verfasst, die mit Unterstützung staatlicher Mittel gewonnen wurden, und ist für die Veröffentlichung der Arbeit in einer ausländischen wissenschaftlichen Zeitschrift die Vorlage der entsprechenden wissenschaftlichen Daten erforderlich?

◯ Ja ◯ Nein

Wenn ja, *hat der Autor der Arbeit die wissenschaftlichen Daten vor der Veröffentlichung der Arbeitgeberin oder dem Arbeitgeber zur einheitlichen Verwaltung vorgelegt?*

◯ Ja ◯ Nein

8.4 Handelt es sich bei den wissenschaftlichen Daten um Staatsgeheimnisse, die Sicherheit des Staates, soziale öffentliche Interessen, Geschäftsgeheimnisse oder personenbezogene Informationen?

◯ Ja ◯ Nein

Falls Offenheit erforderlich ist, wurden die zuständigen Stellen gemäß den Gesetzen und Vorschriften einbezogen?

◯ Ja ◯ Nein

Freifeld für Notizen

Technische und organisatorische Sicherheitsmaßnahmen

9 Erfüllt die Einrichtung in China die erforderlichen technischen Schutzniveaus und Compliance-Anforderungen?

9.1 Hält sich die Einrichtung in China an die allgemeinen Netzsicherheitsverpflichtungen für Netzbetreiber?

◯ Ja ◯ Nein

9.2 Hat das Institut in China eine Selbsteinstufung als Netzbetreiber (MLPS) vorgenommen? Hat eine notwendige Registrierung bei der lokalen PSB stattgefunden?

◯ Ja ◯ Nein

9.3 Ist eine kritische Informationsinfrastruktur (CII) betroffen?

◯ Ja ◯ Nein

9.3.1 Hat der chinesische CII-Betreiber seine besonderen gesetzlichen Verpflichtungen zum Schutz der Sicherheit erfüllt?

◯ Ja ◯ Nein

9.3.2 Hat der chinesische CII-Betreiber die erforderliche Sicherheitsbewertung durch die CAC durchgeführt?

◯ Ja ◯ Nein

9.3.3 Werden personenbezogene Informationen und wichtige Daten generell nur in China gespeichert, es sei denn, eine Sicherheitsbewertung wurde durch die CAC durchgeführt?

◯ Ja ◯ Nein

9.4 Hält sich das Institut in China an die besonderen Anforderungen der NDSM-Bestimmungen zu Netzwerkdaten (besondere Verpflichtungen)?

◯ Ja ◯ Nein

Freifeld für Notizen

Exportkontrolle und Dual-Use

10 **Betrifft das Kooperationsprojekt chinesische Produkte, Dienstleistungen oder Technologien, die als kontrollierte Güter oder Güter mit doppeltem Verwendungszweck eingestuft werden können?**

◯ Ja ◯ Nein

Wenn ja, *und wenn eine Ausfuhr aus China geplant ist: Wurden die erforderlichen Ausfuhrgenehmigungen erteilt?*

◯ Ja ◯ Nein

---

11 **Ist die Einrichtung in Deutschland über verbotene Spionageaktivitäten informiert?**

◯ Ja ◯ Nein

Insbesondere die Einhaltung der älteren ASD-Maßnahmen in Bezug auf Staatsgeheimnisse und wissenschaftliche Daten mit Bezug zur Staatssicherheit verringert potenzielle Risiken. Je proaktiver Einrichtungen in Deutschland mit ihren chinesischen Kolleginnen und Kollegen und den chinesischen Behörden interagieren, indem sie alle Bedenken offen ansprechen, idealerweise schriftlich und im Voraus, desto geringer ist das Risiko späterer potenzieller Vorwürfe. Compliance-Maßnahmen, die unter Berücksichtigung anderer Gesetze ergriffen werden, können dieses Risiko ebenfalls verringern.

Freifeld für Notizen

Umgang mit besonderen Ressourcen

12 **Betrifft das Kooperationsprojekt humangenetische Ressourcen?**

◯ Ja ◯ Nein

Wenn ja, *beachtet die Einrichtung in China die besonderen Anforderungen der HGR-Vorschriften?*

◯ Ja ◯ Nein

13 **Hat das Kooperationsprojekt mit natürlichen Ressourcen zu tun?**

◯ Ja ◯ Nein

Wenn ja, *beachtet die Einrichtung in China die besonderen Anforderungen im Rahmen der NRDS-Maßnahmen?*

◯ Ja ◯ Nein

Freifeld für Notizen

Vertragsgestaltung

14 **Hat die Einrichtung in Deutschland einen ausreichend detaillierten Kooperationsvertrag mit der Einrichtung in China und weitere Vereinbarungen (z. B.Technologie- und Know-how-Lizenzverträge) unterzeichnet, die alle wesentlichen Rechte und Pflichten zwischen den Kooperationspartnern regeln?**

◯ Ja ◯ Nein

14.1 Enthält der Vertrag eine Datentransparenzklausel?

◯ Ja ◯ Nein

14.2 Wurden die Rechte an geistigem Eigentum ausreichend berücksichtigt?

◯ Ja ◯ Nein

14.3 Enthält der Vertrag eine gültige und durchsetzbare Schiedsklausel?

◯ Ja ◯ Nein

Freifeld für Notizen

Herausgeber
Deutscher Akademischer Austauschdienst e.V. (DAAD)
Kennedyallee 50
D-53175 Bonn

Der DAAD ist ein Verein der deutschen Hochschulen und ihrer Studierendenschaften. Er wird institutionell gefördert durch das Auswärtige Amt.

Kompetenzzentrum Internationale Wissenschaftskooperationen (KIWi)

Projektkoordination
Dr. Orane Dornier, Maike Neele Hoffmann, Dr. Christina Philips, DAAD

Redaktion
RÖDL Shanghai
20F Guohua Life Financial Tower
Century Avenue 1501
Shanghai 200122
China

Gestaltung
Atelier Hauer + Dörfler GmbH
Charlottenstraße 17
10117 Berlin

Druck
DAAD, Bonn

1. Auflage, Januar 2026 – 100

Bildnachweis
Titel: deepblue4you/istockphoto

Gefördert durch:

Bundesministerium für Forschung, Technologie und Raumfahrt

Auswärtiges Amt