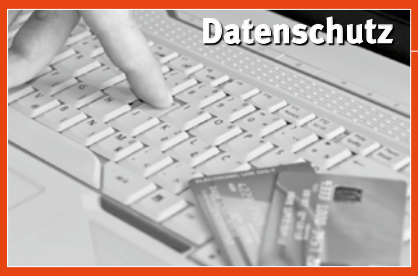
Ausgabe 6 Dezember 2024

Revisionspraxis

PRev

Journal für Revision, IT-Sicherheit, SAP-Sicherheit und Datenschutz



www.prev.de

ISSN 1862-9032

BOORBERG

Inhalt

Karsten Kinast

Datenschutz in Asien: Eine umfassende Analyse von Südkorea, China und Indien

A. Einleitung

In den letzten Jahren hat sich der Datenschutz weltweit zu einem zentralen Anliegen entwickelt, das sowohl Regierungen als auch Unternehmen und Individuen beschäftigt. Besonders in Asien, einer Region, die sich durch ihre dynamische wirtschaftliche Entwicklung und technologische Innovationen auszeichnet, gewinnt der Schutz personenbezogener Daten zunehmend an Bedeutung. China hat sich durch seine rasant wachsende Industrie und technologische Innovationskraft zur zweitgrößten Volkswirtschaft der Welt entwickelt.[1] Besonders die Produktion und der Export von Gütern, zusammen mit dem Ausbau des Technologiesektors, haben China zu einem globalen Wirtschaftsführer gemacht.[2] Südkorea, das sich nach dem Koreakrieg von einem armen Agrarstaat zu einer der führenden Industrienationen Asiens entwickelt hat, ist heute bekannt für seine hochentwickelte Elektronik-, Automobil- und Schiffbauindustrie.[3] Die Wirtschaft Südkoreas zeichnet sich durch eine starke Innovationsfähigkeit und die Dominanz globaler Marken wie beispielsweise Samsung und Hyundai aus.[4] Indien, das sich ebenfalls stark entwickelt hat, ist mittlerweile die fünftgrößte Volkswirtschaft der Welt.[5] Getrieben durch einen boomenden Dienstleistungssektor, insbesondere in der Informationstechnologie, sowie eine wachsende Mittelschicht, hat Indien ein enormes Wirtschaftswachstum erlebt.[6] Die Wirtschaftsreformen der 1990er

1 https://www.tagesschau.de/wirtschaft/konjunktur/china-wirtschaft-wachstum-drittes-quartal-100.html, letzter Zugriff 29.08.2024.
2 https://www.tagesschau.de/wirtschaft/konjunktur/china-wirtschaft-wachstum-drittes-quartal-100.html, letzter Zugriff 29.08.2024.
3 https://www.bmwk.de/Redaktion/DE/Pressemitteilungen/2024/06/20240619-bundesminister-habeck-reise-suedkorea-china.html, letzter Zugriff 29.08.2024.
4 https://www.bmwk.de/Redaktion/DE/Pressemitteilungen/2024/06/20240619-bundesminister-habeck-reise-suedkorea-china.html, letzter Zugriff 29.08.2024.
5 https://www.tagesschau.de/wirtschaft/weltwirtschaft/indien-wachstum-technologie-100.html, letzter Zugriff 29.08.2024.
6 https://www.tagesschau.de/wirtschaft/weltwirtschaft/indien-wachstum-technologie-100.html, letzter Zugriff 29.08.2024.

Jahre und die zunehmende Integration in die Weltwirtschaft haben dazu beigetragen, Indien zu einem wichtigen globalen Akteur zu machen.[7]

Die Vielfalt der rechtlichen und regulatorischen Ansätze der soeben genannten Länder spiegelt die unterschiedlichen politischen, kulturellen und wirtschaftlichen Rahmenbedingungen wider. In diesem Artikel wird eine umfassende Analyse ihrer Datenschutzregulierungen und -praktiken vorgenommen. Dabei werden nicht nur die individuellen Herausforderungen und Fortschritte beleuchtet, sondern auch die Implikationen für den globalen Datenschutzkontext diskutiert. Ziel ist es, ein tieferes Verständnis für die Rolle Asiens im weltweiten Datenschutzdiskurs zu vermitteln und die verschiedenen Herangehensweisen der Länder miteinander zu vergleichen.

B. Südkorea

I. Status Quo des südkoreanischen Datenschutzes

Südkorea gilt im asiatischen Raum als Vorreiter im Datenschutz und hat traditionell strenge Regelungen, die in den letzten Jahren weiter verschärft wurden. Aus diesem Grund wird das Land oft als eine der anspruchsvollsten Jurisdiktionen für internationale Unternehmen im Bereich des Datenschutzes bewertet. Der Personal Information Protection Act (PIPA), der 2011 in Südkorea eingeführt wurde, bildet das Fundament dieser strikten Regulierung. Mit der Einführung des PIPA setzte Südkorea neue Maßstäbe im asiatischen Raum, indem es umfassende und strenge Regelungen für die Erhebung, Verarbeitung und Speicherung von Informationen etablierte. Der PIPA ist darauf ausgerichtet, die Rechte der Bürger zu schützen und sicherzustellen, dass Datenverarbeitungspraktiken transparent und rechtmäßig erfolgen, weshalb die Datenverarbeitung fast ausschließlich auf Basis einer Einwilligung erlaubt ist.

Besonders hervorzuheben sind die umfangreichen und strengen Meldepflichten bei Datenschutzvorfällen sowie die detaillierten Vorgaben für *Technische und Organisatorische Maßnahmen* (TOM), die auf 20 Seiten präzise beschrieben sind. Es ist daher wenig überraschend, dass die EU-Kommission Südkorea seit 2021 als sicheres Drittland anerkennt. Die verpflichtenden Regelungen, die in vielen Bereichen fortschrittlicher und umfassender als die DSGVO sind, zeigen einerseits die Parallelen zum europäischen Ansatz, andererseits, dass Südkorea bereits 2011 ein eigenständiges und strenges Datenschutzrecht entwickelt hat.

7 https://www.tagesschau.de/wirtschaft/weltwirtschaft/indien-wachstum-technologie-100.html, letzter Zugriff 29.08.2024.

II. Struktur und Inhalte des PIPA im Überblick

a. Einwilligungsbasierte Datenverarbeitung

Der Personal Information Protection Act ist das Herzstück des südkoreanischen Datenschutzes. Im Bereich der einwilligungsbasierten Datenverarbeitung fordert der PIPA gemäß Artikel 15 PIPA, dass jede Verarbeitung personenbezogener Daten auf der expliziten Zustimmung der betroffenen Person beruht.[8] Dies bedeutet, dass die betroffenen Personen gemäß Artikel 17 PIPA umfassend informiert werden müssen, bevor ihre Daten verwendet werden können, und dass sie die Freiheit haben, diese Zustimmung jederzeit zu widerrufen.[9] Dieser Prozess stellt sicher, dass die Rechte der Individuen im Mittelpunkt der Datenverarbeitung stehen.

b. Meldepflichten bei Datenschutzvorfällen

Ein weiterer zentraler Bestandteil des PIPA sind die Meldepflichten bei Datenschutzvorfällen, die in Artikel 34 festgelegt sind.[10] Im Falle eines Datenlecks oder einer Verletzung der Datensicherheit sind Unternehmen gesetzlich verpflichtet, die zuständigen Behörden unverzüglich zu informieren.[11] Diese Regelung zielt darauf ab, eine schnelle Reaktion auf Datenschutzverletzungen zu gewährleisten und das Risiko weiterer Schäden zu minimieren.[12] Die betroffenen Personen müssen ebenfalls informiert werden, damit sie geeignete Maßnahmen zum Schutz ihrer Daten ergreifen können.[13]

c. Technische und organisatorische Maßnahmen

Der PIPA legt großen Wert auf technische und organisatorische Maßnahmen zur Sicherung personenbezogener Daten, die in Artikel 29 PIPA detailliert beschrieben sind.[14] Diese Maßnahmen umfassen spezifische Anforderungen wie etwa die Implementierung fortschrittlicher Verschlüsselungstechnologien, die regelmäßige Durchführung von Sicherheitsüberprüfungen und die Schulung von Mitarbeitern im Datenschutz.[15] Diese Maßnahmen sind darauf ausgelegt, die Datensicherheit auf höchstem Niveau zu halten und den Schutz vor unbefugtem Zugriff oder Datenverlust zu maximieren.

8 D 2.164.1 Personal Information Protection Act Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz 94 2024.
9 D 2.164.1 Personal Information Protection Act Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz 94 2024.
10 D 2.164.1 Personal Information Protection Act Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz 94 2024.
11 D 2.164.1 Personal Information Protection Act Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz 94 2024.
12 D 2.164.1 Personal Information Protection Act Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz 94 2024.
13 D 2.164.1 Personal Information Protection Act Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz 94 2024.
14 D 2.164.1 Personal Information Protection Act Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz 94 2024.
15 D 2.164.1 Personal Information Protection Act Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz 94 2024.

d. Vergleich mit der DSGVO: Fortschrittlichkeit und umfassendere Vorschriften

Im Vergleich mit der DSGVO zeigt sich, dass der PIPA in einigen Bereichen sogar weiter geht als das europäische Datenschutzrecht. Während beide Regelwerke hohe Standards für den Datenschutz setzen, ist der PIPA in Bezug auf die Einwilligungsanforderungen und die Ausgestaltung der TOM teilweise strenger.[16]

So sind insbesondere die Bedingungen für die Erhebung und Nutzung personenbezogener Daten zu nennen. Nach Artikel 15 PIPA muss die Einwilligung nicht nur ausdrücklich erteilt werden, sondern auch auf einer umfassenden und detaillierten Information basieren, die den betroffenen Personen bereitgestellt wird.[17] Während die DSGVO ebenfalls eine ausdrückliche Einwilligung verlangt, sieht der PIPA strenge Anforderungen an die Form der Einwilligung vor: Diese muss für jeden spezifischen Zweck der Datenverarbeitung separat eingeholt werden, was in der DSGVO weniger strikt geregelt ist.[18] Die DSGVO erlaubt teilweise die Verarbeitung auf Grundlage berechtigter Interessen ohne Einwilligung, was der PIPA in dieser Form nicht vorsieht.[19]

In Bezug auf die Meldepflichten bei Datenschutzverletzungen ist der PIPA ebenfalls strenger. Während die DSGVO eine Meldefrist von 72 Stunden vorsieht, verlangt Artikel 34 PIPA, dass die Meldung stets „ohne Verzögerung" erfolgt, was in der Praxis zu einer schnelleren Reaktionspflicht führen kann. Außerdem sieht der PIPA höhere Strafen bei Nichteinhaltung dieser Meldepflichten vor.[20]

Im Vergleich zur DSGVO, die ebenfalls hohe Anforderungen an Sicherheitsmaßnahmen stellt, ist der PIPA in Bezug auf die Anforderungen an regelmäßige Audits und die fortlaufende Überwachung und Anpassung der Sicherheitsmaßnahmen umfassender und detaillierter.[21] Die Verantwortung für die Sicherheit der Daten liegt stärker auf der Unternehmensseite, und es werden strengere Vorgaben zur Überprüfung und Dokumentation dieser Maßnahmen gemacht.[22]

Darüber hinaus legt der PIPA besonderen Wert auf die Prävention von Datenschutzverletzungen und verlangt von Unternehmen gemäß Artikel 28 proaktive und umfassende Sicherheitsstrategien zu entwickeln.[23] Diese Fortschrittlichkeit macht Südkorea zu einem der führenden Länder im Datenschutz in Asien und unterstreicht seine Vorreiterrolle in diesem Bereich.

III. Einstufung Südkoreas als sicheres Drittland durch die EU-Kommission

Das südkoreanische Ministerium für Information (MOI) erklärte bereits im Dezember 2015, dass das Land bis zur zweiten Jahreshälfte 2017 den EU-Angemessenheitsstatus anstrebe und gegebenenfalls Gesetze zur Erhöhung des Datenschutzniveaus erlassen werde.[24]

Etwas später als ursprünglich erklärt veröffentlichte der Europäische Datenschutzausschuss (EDSA) am 27. September 2021 seine Stellungnahme zum Entwurf eines Angemessenheitsbeschlusses der EU-Kommission für Südkorea.[25]

Gemäß der DSGVO dürfen personenbezogene Daten nur dann in ein Drittland außerhalb des EWR übermittelt werden, wenn dort ein angemessenes Schutzniveau gewährleistet ist.[26] Ein solches Niveau kann die EU-Kommission durch einen Angemessenheitsbeschluss gemäß Artikel 45 DSGVO feststellen, wodurch die Datenübermittlung in dieses Land ohne zusätzliche Genehmigungen möglich wird.[27]

In seiner Bewertung prüfte nun der EDSA, ob das in Südkorea geltende Datenschutzniveau mit dem der DSGVO vergleichbar ist.[28] Dabei konzentrierte sich der Ausschuss insbesondere auf den dortigen rechtlichen Rahmen bezüglich allgemeiner Datenschutzgrundsätze, die Möglichkeiten staatlicher Behörden, auf personenbezogene Daten zuzugreifen, sowie die Rechtsbehelfe für betroffene Personen.[29] Der EDSA kam zu dem Schluss, dass viele zentrale Elemente des koreanischen Datenschutzsystems im Wesentlichen den EU-Standards entsprechen.[30] Dennoch empfahl der Ausschuss der EU-Kommission, bestimmte Punkte weiter zu untersuchen. Nach einer detaillierten Analyse des südkoreanischen Rechtssystems kam die Kommission zu dem Ergebnis, dass dieses im Wesentlichen ein mit der

16 D 2.164.1 Personal Information Protection Act Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz 94 2024.
17 D 2.164.1 Personal Information Protection Act Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz 94 2024.
18 D 2.164.1 Personal Information Protection Act Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz 94 2024.
19 D 2.164.1 Personal Information Protection Act Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz 94 2024.
20 D 2.164.1 Personal Information Protection Act Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz 94 2024.
21 D 2.164.1 Personal Information Protection Act Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz 94 2024.
22 D 2.164.1 Personal Information Protection Act Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz 94 2024.
23 D 2.164.1 Personal Information Protection Act Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz 94 2024.
24 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 35.
25 Etteldorf: EDSA: Datenschutzrechtliche Angemessenheitsentscheidung für Südkorea ZD-Aktuell 2021, 05506.
26 Etteldorf: EDSA: Datenschutzrechtliche Angemessenheitsentscheidung für Südkorea ZD-Aktuell 2021, 05506.
27 Etteldorf: EDSA: Datenschutzrechtliche Angemessenheitsentscheidung für Südkorea ZD-Aktuell 2021, 05506.
28 Etteldorf: EDSA: Datenschutzrechtliche Angemessenheitsentscheidung für Südkorea ZD-Aktuell 2021, 05506.
29 Etteldorf: EDSA: Datenschutzrechtliche Angemessenheitsentscheidung für Südkorea ZD-Aktuell 2021, 05506.
30 Etteldorf: EDSA: Datenschutzrechtliche Angemessenheitsentscheidung für Südkorea ZD-Aktuell 2021, 05506.

DSGVO vergleichbares Datenschutzniveau bietet, ergänzt durch verbindliche Zusagen und Erläuterungen seitens Südkoreas.[31] Der EDSA stellte positiv fest, dass wesentliche Garantien des EU-Datenschutzrechts auch in Südkorea vorhanden sind, insbesondere in Bezug auf rechtmäßige Verarbeitung, Zweckbindung, Datensicherheit und Transparenz.[32] Gleichzeitig bat der EDSA die Kommission, weitergehende Informationen über die Verbindlichkeit und Durchsetzbarkeit der Zusagen Südkoreas einzuholen und empfahl eine sorgfältige Überwachung dieser Aspekte in der Praxis.[33] Zudem äußerte der EDSA weiteren Informationsbedarf bezüglich der Wirksamkeit von Rechtsbehelfen für EU-Bürger und betonte, dass die Kommission die Bedingungen für Beschwerden und Klagen im südkoreanischen System genauer prüfen solle.[34]

Hinsichtlich des Zugriffs staatlicher Behörden auf personenbezogene Daten stellte der EDSA fest, dass das südkoreanische Datenschutzgesetz auch im Bereich der Strafverfolgung gilt und dass Sonderregelungen zum Schutz der nationalen Sicherheit bestehen, diese jedoch ebenfalls grundlegende Prinzipien und Überwachungsmechanismen beinhalten.[35] Abschließend stimmte der EDSA der Einschätzung der Kommission zu, dass Südkorea über ein unabhängiges und effektives Überwachungssystem verfügt.[36]

Am 17. Dezember 2021 hat die EU-Kommission gemäß Artikel 45 Absatz 3 DSGVO nach Abschluss der Evaluation festgestellt, dass in Südkorea ein angemessenes Datenschutzniveau nach EU-Standards gewährleistet ist.[37]

IV. Datenschutzvorfälle und deren Verfolgung

Zuständig als regulatorische Aufsicht für den Datenschutz ist die Personal Information Protection Commission (PIPC). Hinsichtlich der Verfolgung von Datenschutzverstößen und der Durchsetzung des nationalen Datenschutzrechts kann Korea einen Erfolg verzeichnen. Das liegt unter anderem an dem strengen Sanktionskatalog in Kapitel 9 des PIPA, der Geldstrafen in Höhe von bis zu 3 % des Gesamtumsatzes des Zuwiderhandelnden und sogar Freiheitsstrafen von bis zu fünf Jahren vorschreibt[38]. Gerichten steht es zu, wenn der Verantwortliche sein vorsätzliches oder grob fahrlässiges Handeln nicht widerlegen kann, den Schadensersatz dreimal höher als den tatsächlichen Schaden anzusetzen.[39] So erließ die PIPC beispielsweise erst im Frühjahr 2024 ein Rekordbußgeld in Höhe von 15 Billionen KRW (ca. 10 Millionen Euro) gegen ein Unternehmen wegen PIPA-Verletzungen. Das Unternehmen hatte keine hinreichenden Sicherheitsvorkehrungen zum Schutz personenbezogener Daten ergriffen, sodass diese zum illegalen Datenhandel verfügbar waren.[40] Zur effizienteren Verfahrensschlichtung gibt es Mediationsverfahren und hinsichtlich Unterlassungsansprüchen Sammelklagen.[41]

V. Zwischenfazit Südkorea

Südkorea hat sich als Vorreiter im asiatischen Datenschutz etabliert, insbesondere durch die Einführung und kontinuierliche Verbesserung des „Personal Information Protection Act“. Mit strengen Datenschutzregelungen, die denen der EU-Datenschutz-Grundverordnung ähneln und der Einrichtung einer unabhängigen Datenschutzaufsichtsbehörde setzt Südkorea hohe Standards im Schutz personenbezogener Daten. Diese Bemühungen wurden 2021 durch die Anerkennung eines angemessenen Datenschutzniveaus durch die Europäische Kommission bestätigt, was die internationale Vorreiterrolle Südkoreas im Bereich Datenschutz weiter festigte.

C. China

I. Status Quo des chinesischen Datenschutzes unter Berücksichtigung Hongkongs

In den letzten Jahren hat China erhebliche Anstrengungen unternommen, um den Schutz von Informationen zu verbessern.[42] Während das chinesische Datenschutzrecht 2019 noch wenig entwickelt war[43], wurden seit 2021 bedeutende Fortschritte erzielt, insbesondere durch die Einführung des neuen Datensicher-

31 Etteldorf: EDSA: Datenschutzrechtliche Angemessenheitsentscheidung für Südkorea ZD-Aktuell 2021, 05506.
32 Etteldorf: EDSA: Datenschutzrechtliche Angemessenheitsentscheidung für Südkorea ZD-Aktuell 2021, 05506.
33 Etteldorf: EDSA: Datenschutzrechtliche Angemessenheitsentscheidung für Südkorea ZD-Aktuell 2021, 05506.
34 Etteldorf: EDSA: Datenschutzrechtliche Angemessenheitsentscheidung für Südkorea ZD-Aktuell 2021, 05506.
35 Etteldorf: EDSA: Datenschutzrechtliche Angemessenheitsentscheidung für Südkorea ZD-Aktuell 2021, 05506.
36 Etteldorf: EDSA: Datenschutzrechtliche Angemessenheitsentscheidung für Südkorea ZD-Aktuell 2021, 05506.
37 https://legal.pwc.de/de/news/fachbeitraege/eu-angemessenheitsbeschluss-zu-suedkorea#:~:text=Dezember%202021%20hat%20die%20Europ%C3%A4ische,der%20Evaluierung%20durch%20die%20Kommission, letzter Zugriff am 03.09.2024.
38 https://www.activemind.legal/de/guides/pipa-suedkorea/; letzter Zugriff am 17.09.2024.
39 https://www.activemind.legal/de/guides/pipa-suedkorea/; letzter Zugriff am 17.09.2024.
40 https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=10180#LINK; letzter Zugriff am 23.09.2024.
41 https://www.activemind.legal/de/guides/pipa-suedkorea/; letzter Zugriff am 17.09.2024.
42 Johannes, ZD 2022, 90.
43 Simitis/Hornung/Spiecker gen. Döhmann/Hornung/Spiecker gen. Döhmann, 1. Auflage 2019, Datenschutzrecht, Einleitung Rn. 258.

heitsgesetzes (Data Security Law (DSL)) und des Gesetzes zum Schutz persönlicher Informationen (Personal Information Protection Law (PIPL)). Diese Gesetze haben eine umfassende Regulierung etabliert, die in vielen Aspekten starke Ähnlichkeiten zur DSGVO aufweist.

Die Volksrepublik China verfügte in der Vergangenheit über weite Strecken nicht über ein umfassendes Datenschutzgesetz.[44] Es existierten jedoch spezielle Regelungen für die Erhebung und Nutzung von Daten im Bankensektor, die im Zusammenhang mit Chinas Beitritt zur WHO stehen.[45] Anbieter von Webseiten und E-Mail-Diensten sind verpflichtet, die Inhalte vertraulich zu behandeln, müssen jedoch auf Anfrage ihre Daten an Sicherheitsbehörden weitergeben.[46]

Am 1. Juli 2017 trat das chinesische Cybersicherheitsgesetz in Kraft, das international viel Kritik erfuhr.[47] Es war das erste umfassende Gesetz in China, das Unternehmen vorschrieb, wie sie digitale Informationen verwalten und schützen müssen.[48] Das Gesetz legt strenge Beschränkungen für den Export bestimmter Daten aus China fest, wobei die Regierung vor dem Export Zugang zu diesen Daten haben muss.[49] Für internationale Unternehmen waren die neuen Regelungen, die die Speicherung bestimmter Daten in China sowie die obligatorische Sicherheitsbewertung durch die Aufsichtsbehörden für den Export wichtiger Daten verlangen, nur schwer akzeptabel.[50] Trotz Protesten von Unternehmensseite blieb das Gesetz bestehen.[51]

Hongkong, seit dem 1. Juli 1997 Sonderverwaltungsregion der Volksrepublik China und gemäß der chinesischen Verfassung der Zentralregierung in Peking unterstehend[52], verfügt hingegen über ein ausgefeiltes Datenschutzgesetz: Die Personal Data (Privacy) Ordinance (PDPO) von 1995, die noch auf britischem Recht basiert.[53] Dieses Gesetz wird durch den Privacy Commissioner, die erste asiatische Datenschutzbehörde, durchgesetzt.[54] Allerdings wird die praktische Durchsetzungskraft der Behörde in Frage gestellt, da der Privacy Commissioner auch nach einer Reform keine Strafen verhängen kann.[55]

Insbesondere das PIPL zeigt in seiner Regelungssystematik Parallelen zur DSGVO[56] geht jedoch in Bezug auf internationalen Datenverkehr und Datenlokalisierung sogar noch weiter. Bemerkenswert ist auch, dass das chinesische Recht keine Unterscheidung zwischen Verantwortlichen und Auftragsverarbeitern macht, wie es in der DSGVO der Fall ist. Darüber hinaus enthält das chinesische Datenschutzrecht eine Reihe von Bestimmungen, die in der DSGVO keine Entsprechung finden.[57] Insgesamt zeigt sich, dass der individuelle Schutz oft zugunsten nationaler Interessen zurücktritt.[58]

II. Überblick über die Einführung des Cybersicherheitsgesetzes (CSL), des Datensicherheitsgesetzes (DSL) und des Gesetzes zum Schutz persönlicher Informationen (PIPL)

1. Cybersicherheitsgesetz (CSL)

Seit dem 1. Juni 2017 ist in China das Cybersicherheitsgesetz in Kraft, das vorschreibt, dass Unternehmen relevante Daten innerhalb Chinas speichern müssen.[59] Der Export dieser Daten ist nur unter bestimmten Bedingungen erlaubt.[60] Dieses Gesetz richtet sich insbesondere an Betreiber von Netzwerken, einschließlich internationaler Unternehmen, die in China tätig sind.[61]

2. Datensicherheitsgesetz (DSL)

Ab dem 1. September 2021 trat in China das neue Datensicherheitsgesetz in Kraft.[62] Dieses Gesetz, das am 10. Juni 2021 vom Ständigen Ausschuss des Nationalen Volkskongresses verabschiedet wurde, bringt zusätzliche Komplexität in das chinesische Rechtssystem.[63] Es

44 Übersicht: BNA World Data Protection Report („World Report"), 11/2008, S. 21 ff.
45 Ins. 1995 Commercial Banking Law sowie den damit verbundenen Verwaltungsanordnungen, BNA World Report, 11/2008, S. 22.
46 BNA World Report, 11/2008, S. 23.
47 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 28.
48 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 28.
49 FT Cyber Security, „China's cyber security law rattles multinationals", Financial Times v. 30. 5. 2017, abrufbar unter https://www.ft.com/content/b302269c-44ff-11e7–8519-9f94ee97d996 (Stand: 2/2018).
50 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 29.
51 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 29.
52 https://www.auswaertiges-amt.de/de/service/laender/hongkong-node/politisches-portraet/200956, letzter Zugriff 03.09.2024.
53 https://www.pcpd.org.hk/ (Stand: 2/2018).
54 Zuletzt *Greenleaf/McLeish*, PL&B International (Ausgabe 116) 4/2012, 25.
55 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 31.
56 Johannes, ZD 2022, 90 (92 ff.).
57 Vgl. Johannes, ZD 2022, 90 (97f.).
58 Johannes, ZD 2022, 90 (98).
59 https://www.ihk.de/pfalz/international/greater-china/china/china-recht-und-steuern/datensicherheitsgesetz-china-5239572; letzter Zugriff 03.09.2024.
60 https://www.ihk.de/pfalz/international/greater-china/china/china-recht-und-steuern/datensicherheitsgesetz-china-5239572; letzter Zugriff 03.09.2024.
61 https://www.ihk.de/pfalz/international/greater-china/china/china-recht-und-steuern/datensicherheitsgesetz-china-5239572; letzter Zugriff 03.09.2024.
62 https://www.ihk.de/pfalz/international/greater-china/china/china-recht-und-steuern/datensicherheitsgesetz-china-5239572; letzter Zugriff 03.09.2024.
63 https://www.ihk.de/pfalz/international/greater-china/china/china-recht-und-steuern/datensicherheitsgesetz-china-5239572; letzter Zugriff 03.09.2024.

führt Konzepte wie „wichtige Daten“ und „Schlüsseldaten“ ein und legt strenge Sicherheitsmaßnahmen fest.[64] Diese Entwicklungen deuten darauf hin, dass weitere unterstützende Vorschriften, wie beispielsweise „wichtige Datenkataloge“, folgen könnten.[65]

3. Gesetz zum Schutz persönlicher Informationen (PIPL)

Das Gesetz zum Schutz persönlicher Informationen, das am 1. November 2021 in Kraft trat, ist Chinas erstes umfassendes Gesetz zum Schutz personenbezogener Daten.[66] Es regelt die Verarbeitung persönlicher Informationen einschließlich ihrer Erhebung, Speicherung, Nutzung, Verarbeitung, Übermittlung, Bereitstellung, Veröffentlichung und Löschung.[67] Das Gesetz hat eine extraterritoriale Wirkung, da es auch auf die Verarbeitung von Daten natürlicher Personen in China anwendbar ist, selbst wenn diese außerhalb des Landes erfolgt.[68] Das PIPL wird oft als die „chinesische Datenschutzgrundverordnung“[69] bezeichnet, da es den Schutz individueller Rechte ähnlich wie die europäische DSGVO stärkt, wobei es jedoch auch einige wesentliche Unterschiede gibt (Näheres unter C.III.).

Diese Gesetze signalisieren Chinas wachsenden Anspruch, den Datenschutz auf nationaler Ebene zu stärken, während gleichzeitig die Kontrolle über Daten im Rahmen der nationalen Sicherheitsinteressen erhöht wird.

III. Wesentliche Bestimmungen des PIPL

1. Grundprinzipien und Ähnlichkeiten zur DSGVO

Das PIPL führt in China zum ersten Mal zum umfassenden Schutz personenbezogener Daten, indem der Datenmissbrauch durch private Unternehmen unterbunden wird. Der Begriff der personenbezogenen Daten ist im chinesischen Recht ähnlich weit gefasst wie in der DSGVO und umfasst somit auch Informationen mit einfachem Personenbezug wie etwa IP-Adressen.[70] Ebenso finden sich auch mit Artikel 5 DSGVO vergleichbare allgemeine Grundsätze wie die Zweckbindung und Datenminimierung im PIPL wieder.[71] Des Weiteren bedarf es für die Rechtmäßigkeit der Datenverarbeitung einer Rechtsgrundlage, die sich ähnlich wie nach der DSGVO etwa aus einer Einwilligung oder dem Gesetz ergeben kann. Anders ist jedoch, dass bereits von der Person oder auf sonstige Weise offengelegte Informationen nicht zwangsläufig einer Einwilligung bedürfen.[72] Zudem gibt es auch im chinesischen Datenschutzrecht besondere Datenkategorien, die einen speziellen Schutz erhalten.[73] Auch gibt es verschiedene Betroffenenrechte und Informationspflichten. Für die Auftragsverarbeitung bestehen vergleichbare Regelungen wie in Artikel 28 DSGVO.[74]

Die Prinzipien in den Artikeln 5 bis 9 des PIPL sind stark an die Regelungen in Art. 5 der DSGVO angelehnt.[75] Gemäß Art. 5 des PIPL muss die Datenverarbeitung rechtmäßig und in guter Absicht erfolgen, was dem Grundsatz von Treu und Glauben in Art. 5 Abs. 1 lit. a der DSGVO entspricht.[76] Der Transparenzgrundsatz wird in Art. 7 PIPL geregelt.[77] Art. 6 PIPL fordert zudem die Zweckbindung und Datenminimierung, was den Regelungen in Art. 5 Abs. 1 lit. b und lit. c der DSGVO ähnlich ist.[78] Darüber hinaus verlangt Art. 8 PIPL die Sicherstellung der Datenqualität, um negative Auswirkungen auf Rechte und Interessen der betroffenen Personen durch ungenaue oder unvollständige Daten zu vermeiden – ein Prinzip, das auch im Grundsatz der Richtigkeit in Art. 5 Abs. 1 lit. d der DSGVO verankert ist.[79] Art. 9 PIPL betont die persönliche Verantwortung der Datenverarbeiter, einschließlich der Notwendigkeit von Datensicherheitsmaßnahmen, was dem Grundsatz der Sicherheit in Art. 5 Abs. 1 lit. d und Art. 24 der DSGVO entspricht.[80] Der Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e der DSGVO findet seine Parallele in Art. 19 PIPL.[81]

2. Unterschiede: Internationale Datenübertragung und Datenlokalisierung

Die DSGVO und das PIPL weisen einige Parallelen auf. Es gibt aber auch einige bedeutsame Unterschiede. Besonders bemerkenswert ist zunächst die Tatsache, dass

64 https://www.ihk.de/pfalz/international/greater-china/china/china-recht-und-steuern/datensicherheitsgesetz-china-5239572; letzter Zugriff 03.09.2024.
65 https://www.ihk.de/pfalz/international/greater-china/china/china-recht-und-steuern/datensicherheitsgesetz-china-5239572; letzter Zugriff 03.09.2024.
66 https://www.ihk.de/pfalz/international/greater-china/china/china-recht-und-steuern/datensicherheitsgesetz-china-5239572; letzter Zugriff 03.09.2024.
67 https://www.ihk.de/pfalz/international/greater-china/china/china-recht-und-steuern/datensicherheitsgesetz-china-5239572; letzter Zugriff 03.09.2024.
68 https://www.ihk.de/pfalz/international/greater-china/china/china-recht-und-steuern/datensicherheitsgesetz-china-5239572; letzter Zugriff 03.09.2024.
69 https://www.ihk.de/pfalz/international/greater-china/china/china-recht-und-steuern/datensicherheitsgesetz-china-5239572;letzter Zugriff 03.09.2024.
70 https://www.activemind.legal/de/guides/pipl/; letzter Zugriff am 17.09.2024.
71 https://www.activemind.legal/de/guides/pipl/; letzter Zugriff am 17.09.2024.
72 https://www.activemind.legal/de/guides/pipl/; letzter Zugriff am 17.09.2024.
73 https://www.activemind.legal/de/guides/pipl/; letzter Zugriff am 17.09.2024.
74 https://www.activemind.legal/de/guides/pipl/; letzter Zugriff am 17.09.2024.
75 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.
76 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.
77 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.
78 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.
79 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.
80 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.
81 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.

das PIPL primär nur für Privatunternehmen gilt und öffentliche Stellen grundsätzlich ausgenommen sind.[82] Konsequent hierzu stellen die Rechte auf Privatsphäre und Datenschutz auch keine Grundrechte dar, weshalb der Staat weiterhin die Befugnis zu einer umfangreichen Überwachung hat.[83] Auch ist die chinesische Aufsichtsbehörde anders als europäische Datenschutzbehörden (vgl. Artikel 52 DSGVO) nicht unabhängig aufgebaut.[84] Eine Besonderheit besteht auch hinsichtlich der Sanktionen. Die Bußgelder können nämlich nicht nur gegen juristische Personen als "Verantwortliche", sondern auch gegen direkt verantwortliche Personen und Mitarbeiter in Höhe von 100.000 und eine Millionen Yuan verhängt werden.[85] Auch kann für entsprechende Personen ein Tätigkeitsverbot erlassen werden.[86]

Der Geltungsbereich knüpft nicht ausschließlich an eine territoriale Datenverarbeitung wie nach der DSGVO an, sondern geht über diesen Bereich hinaus.[87] Das Gesetz gilt nach Artikel 3 PIPL immer auch dann, wenn im Ausland personenbezogene Daten von chinesischen Bürgern verarbeitet werden, wenn dies der Bereitstellung von Produkten oder Dienstleistungen oder der Analyse des Verhaltens dient.[88] In China gibt es zudem spezielle Vorgaben zum grenzüberschreitenden Datenverkehr in Verbindung mit dem CSL, die eine Pflicht zur Datenlokalisierung in China vorschreiben. Das bedeutet, dass Daten, die übertragen werden sollen, auch lokal innerhalb der chinesischen Staatsgrenzen gespeichert werden müssen.

Für einen rechtmäßigen Auslandstransfer muss dann entweder die Sicherheitsprüfung durch eine spezielle Stelle stattfinden, oder es sind Standardvertragsklauseln zu verwenden.[89]

IV. Aufsicht

Kapitel 6 des PIPL enthält mit der DSGVO vergleichbare Bestimmungen zur staatlichen Überwachung. In Art. 59 PIPL wird die Einrichtung spezialisierter sowie regionaler Aufsichtsbehörden gefordert, deren Aufgaben und Befugnisse in den Artikeln 60, 61 und 63 bis 64 PIPL festgelegt sind.[90] Die Koordination dieser Behörden übernimmt die Cyberspace Administration of China (CAC).[91] Eine besondere Bedeutung kommt der CAC gemäß Art. 62 PIPL zu, da sie für die Ausarbeitung konkreter Vorschriften und Standards zum Schutz personenbezogener Daten verantwortlich ist.[92] Dies umfasst auch spezielle Regelungen für neue Technologien und Anwendungen wie Gesichtserkennung und Künstliche Intelligenz, insbesondere in Bezug auf personenbezogene Daten.[93] Nach Art. 61 Nr. 4 PIPL in Verbindung mit Art. 63 PIPL haben die Aufsichtsbehörden umfassende Befugnisse, um illegale Aktivitäten bei der Verarbeitung personenbezogener Daten zu untersuchen.[94] Zudem können sie gemäß Art. 64 PIPL Abhilfemaßnahmen ergreifen und nach Art. 66 f PIPL Bußgelder sowie andere Sanktionen verhängen.[95] Bemerkenswert ist in diesem Kontext etwa das Rekordbußgeld gegen den App-basierten Mobilitätsanbieter Didi Global aus dem Jahr 2022 in Höhe von damals 1,16 Milliarden Euro. Die CAC warf dem Unternehmen mit Sitz auf den Cayman Inseln im Rahmen der extraterritorialen Geltung des PIPL vor, unter anderem illegal und in großem Ausmaß Daten von Nutzern gesammelt zu haben.

V. Angemessenheitsbeschluss

Das PIPL weist in seiner Konzeption und seinem Umfang Ähnlichkeiten mit der DSGVO auf und kann ebenfalls als umfassend betrachtet werden.[96] Allerdings zielt das Gesetz vorrangig darauf ab, personenbezogene Daten vor den negativen Auswirkungen eines unregulierten chinesischen Technologiesektors zu schützen anstatt vor unverhältnismäßigen Eingriffen durch staatliche Behörden.[97] Aufgrund des politischen Systems in China bietet es nur begrenzten Schutz gegen die Bedrohungen, die von einem übergreifenden Si-

82 https://www.ihk.de/stuttgart/fuer-unternehmen/international/internationales-wirtschaftsrecht/rechtsinformationen-zu-einzelnen-laendern/asien/das-neue-chinesischen-datenschutzgesetz-pipl-5279868; letzter Zugriff am 17.09.2024.
83 https://www.activemind.legal/de/guides/pipl/; letzter Zugriff am 17.09.2024.
84 https://www.activemind.legal/de/guides/pipl/, letzter Zugriff am 17.09.2024.
85 https://www.activemind.legal/de/guides/pipl/; letzter Zugriff am 17.09.2024.
86 https://www.activemind.legal/de/guides/pipl/; letzter Zugriff am 17.09.2024.
87 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.
88 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90, https://www.ihk.de/stuttgart/fuer-unternehmen/international/internationales-wirtschaftsrecht/rechtsinformationen-zu-einzelnen-laendern/asien/das-neue-chinesischen-datenschutzgesetz-pipl-5279868; letzter Zugriff am 17.09.2024.
89 https://www.pwc.de/de/internationale-maerkte/firmengruendung-im-ausland/china-business-group/digitalisierung-unter-verschaerften-it-gesetzen.html; letzter Zugriff am 17.09.2024.
90 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.
91 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.
92 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.
93 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.
94 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.
95 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.
96 Eisenmenger: Durchführung von Transfer Impact Assessments am Beispiel der VR China (ZD 2023, 204).
97 Eisenmenger: Durchführung von Transfer Impact Assessments am Beispiel der VR China (ZD 2023, 204)

cherheitsapparat für die individuellen Grundrechte ausgehen.[98]

Eine unabhängige Aufsichtsbehörde, die datenschutzrechtliche Vorschriften auch gegenüber staatlichen Institutionen durchsetzen könnte, existiert nicht.[99] Zudem trägt der Stand der Rechtsstaatlichkeit, angesichts erheblicher Unterschiede in der Rechtskultur und im Rechtsverständnis, wenig zur Verbesserung des Ergebnisses bei.[100] Um personenbezogene Daten sicher nach China zu übermitteln, sind daher zusätzliche Maßnahmen erforderlich, die über die in den Standardvertragsklauseln festgelegten Vorgaben hinausgehen, um ein im Wesentlichen gleichwertiges Schutzniveau wie in Europa zu gewährleisten.[101]

VI. Zwischenfazit China

China hat in den letzten Jahren erhebliche Fortschritte im Bereich des Datenschutzes gemacht. Die chinesischen Gesetze weisen starke Ähnlichkeiten zur DSGVO auf, enthalten jedoch auch deutliche Unterschiede.[102] Besonders hervorzuheben ist die weitreichende Extraterritorialität[103] des PIPL. Allerdings bleibt der Datenschutz in China zugunsten nationaler Interessen eingeschränkt, insbesondere da öffentliche Stellen von vielen Datenschutzregelungen ausgenommen sind.[104] Ein wesentliches Unterscheidungsmerkmal zum europäischen Datenschutz sind zudem die Pflicht zur Datenlokalisierung und die strenge Kontrolle des internationalen Datenverkehrs.[105] Chinas Datenschutzansatz hat erheblichen Einfluss auf den globalen Datenschutzkontext, da internationale Unternehmen, die in China tätig sind, umfangreiche Compliance-Anforderungen erfüllen müssen. Die Ausrichtung des chinesischen Datenschutzrechts zeigt, dass der Schutz individueller Rechte hinter staatlichen Interessen zurücktritt und verdeutlicht die Herausforderungen für globale Datenschutzstandards in einem zunehmend digitalisierten und geopolitisch geprägten Umfeld.

98 Eisenmenger: Durchführung von Transfer Impact Assessments am Beispiel der VR China (ZD 2023, 204).
99 Eisenmenger: Durchführung von Transfer Impact Assessments am Beispiel der VR China (ZD 2023, 204).
100 Eisenmenger: Durchführung von Transfer Impact Assessments am Beispiel der VR China (ZD 2023, 204).
101 Eisenmenger: Durchführung von Transfer Impact Assessments am Beispiel der VR China (ZD 2023, 204).
102 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.
103 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.
104 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.
105 Johannes: Datenschutz und Datensicherheit in China ZD 2022, 90.

D. Indien

I. Status Quo des indischen Datenschutzes

In Indien wird schon seit längerer Zeit an einer datenschutzrechtlichen Gesetzesinitiative gearbeitet, die sich an der Europäischen DSGVO orientieren soll. Dies zeigt sich unter anderem an geplanten Regelungen zu Meldepflichten, erweiterten Rechten für Betroffene und einem internationalen Anwendungsbereich. Allerdings waren die bisherigen Versuche, eine umfassende Datenschutzgesetzgebung zu verabschieden, nicht erfolgreich. Die Herausforderung lag dabei vor allem darin, die Interessen der Zivilgesellschaft mit denen der Wirtschaft in Einklang zu bringen. Zudem zeichnet sich in Indien ein zunehmender Trend zur Betonung von Datenlokalisierung und Datensouveränität ab.

Es ist zu beobachten, dass der politische Konsens darüber wächst, dass eine datenschutzrechtliche Gesetzgebung erforderlich ist, insbesondere um die bedeutende indische Outsourcing-Industrie zu schützen und zu fördern, die immer wieder wegen Sicherheitslücken in die Kritik geraten ist.[106] Berichten zufolge sollen beispielsweise Bankdaten aus Europa, die über indische Call-Center zugänglich waren, in Indien zum Kauf angeboten worden sein.[107] Im Jahr 2006 wurde im Parlament in Delhi ein Entwurf für einen "Personal Data Protection Act" eingebracht, jedoch letztlich nicht verabschiedet.[108] Eine im Auftrag der EU-Kommission durchgeführte Studie kam 2010 zu dem Ergebnis, dass das bestehende Regulierungssystem in Indien nicht ausreichend sei, um den Schutz personenbezogener Daten aus der EU zu gewährleisten.[109] Die indische Industrie hat daraufhin den Data Security Council of India gegründet, ein Gremium, das Selbstregulierung auf Grundlage internationaler Best Practices fördert und sich regelmäßig mit internationalen Organisationen austauscht.[110]

Der Information Technology Act wurde im Jahr 2000 verabschiedet, um E-Commerce zu fördern.[111] Das Gesetz enthält Bestimmungen zu digitalen Signaturen und legt Strafen für Hacking, Virenbefall und andere Computervergehen fest.[112] Zudem verlangt es die Offenlegung von Verschlüsselungsschlüsseln und sieht

106 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 23.
107 Financial Times v. 3. 9. 2011 („UK Financial Data Sold in India, Report Says").
108 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 23.
109 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 23.
110 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 23.
111 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 25.
112 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 25.

hohe Strafen für Verstöße gegen Vertraulichkeit und Privatsphäre im geschäftlichen Umfeld vor.[113]

Im Jahr 2005 trat der Right to Information Act in Kraft, der Einzelpersonen allgemeine Auskunftsrechte gegenüber der Zentralregierung und staatlichen Behörden einräumt.[114] Das Gesetz führte zur Gründung mehrerer Informationskommissionen im ganzen Land, wobei die Zentrale Informationskommission in Delhi die Einführung eines Datenschutzgesetzes unterstützt und möglicherweise als Durchsetzungsbehörde für ein solches Gesetz fungieren könnte.[115]

Eine Datenschutzgesetzgebung („Privacy Bill") vom 19. April 2011, die unter anderem die Einrichtung einer dreiköpfigen Datenschutzkommission vorsieht, wurde in Indien diskutiert.[116] Im April 2011 verabschiedete Indien neue datenschutzrechtliche Bestimmungen auf Basis des Information Technology Act von 2000.[117] Diese „Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011" gelten für alle Organisationen, die in Indien personenbezogene Daten erheben und verarbeiten.[118] Besonders relevant für ausländische Unternehmen ist die darin enthaltene Regel 7, die es Organisationen erlaubt, personenbezogene Daten an Dritte außerhalb Indiens zu übertragen, sofern der Empfänger ein vergleichbares Datenschutzniveau gewährleistet, wie es nach indischem Recht erforderlich ist.[119] Der Datentransfer ins Ausland ist zudem zulässig, wenn er zur Erfüllung eines rechtmäßigen Vertrags notwendig ist oder die betroffene Person dem Transfer zugestimmt hat.[120] Zu den „sensiblen"[121] Daten zählen unter anderem Finanzinformationen, Passwörter, Daten zum physischen, physiologischen und psychischen Gesundheitszustand, sexuelle Orientierung, medizinische Aufzeichnungen und biometrische Daten. Unter Umständen ist die Einholung der Zustimmung der betroffenen Personen erforderlich.[122] Für in Europa ausgelagerte Daten soll dieses Zustimmungserfordernis jedoch nicht gelten, so das indische Ministerium.[123]

Am 24. August 2017 entschied der Oberste Gerichtshof Indiens im Fall Puttaswamy/Union of India[124] einstimmig, dass die indische Verfassung ein unveräußerliches und inhärentes Recht auf Privatsphäre als grundlegendes Verfassungsprinzip anerkennt. Obwohl das Recht auf Privatsphäre nicht ausdrücklich in der Verfassung erwähnt wird, betrachteten die Richter es als abgeleitetes Recht, das durch den Schutz von Leben und Freiheit in Artikel 21 der Verfassung impliziert und durch weitere verfassungsrechtliche Bestimmungen, die Verfahrensgarantien für Bürger enthalten, geschützt wird.[125] Zudem forderte der Gerichtshof den Schutz der Privatsphäre aufgrund der Ratifizierung des Internationalen Pakts über bürgerliche und politische Rechte (IPBPR) der Vereinten Nationen durch Indien, dessen Artikel 17 die Privatsphäre schützt.[126]

II. Aktuelle Entwicklungen und Gesetzesinitiativen

1. Geplante datenschutzrechtliche Gesetzesinitiativen, inspiriert von der DSGVO

Nachdem die indische Regierung am 3. August 2022 den Entwurf des Data Protection Bill von 2019 zurückgezogen hatte, veröffentlichte das indische Ministerium für Elektronik und Informationstechnologie am 18. November 2022 einen neuen, kürzeren Entwurf unter dem Titel Digital Personal Data Protection Bill 2022 (DPDP Bill, 2022).[127] Dieser Entwurf soll als Grundlage für umfassende Datenschutzregelungen in Indien dienen.[128]

2. Erstes Datenschutzgesetz verabschiedet

Am 11. August 2023 wurde der Digital Personal Data Protection Act, 2023 (DPDP Act) von der indischen Staatspräsidentin genehmigt.[129] Damit hat Indien sein erstes eigenständiges Datenschutzgesetz verabschiedet.

Der Digital Personal Data Protection Act, 2023 (DPDP Act) stellt ein Rahmengesetz zum Schutz digita-

113 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 25.
114 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 25.
115 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 25.
116 http://bourgeoisinspirations.files.wordpress.com/2010/03/draft_right-to-privacy.pdf (Stand: 3/2016).
117 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 26.
118 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 26.
119 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 26.
120 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 26.
121 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 26.
122 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 26.
123 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 26.
124 http://bourgeoisinspirations.files.wordpress.com/2010/03/draft_right-to-privacy.pdf (Stand: 3/2016).
125 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 27.
126 Spies in Spies Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 3. Auflage 2019 Rn. 27.
127 https://www.activemind.legal/de/guides/indien-dpdp/; letzter Zugriff am 19.09.2024.
128 https://www.activemind.legal/de/guides/indien-dpdp/; letzter Zugriff am 19.09.2024.
129 https://www.gtai.de/de/trade/indien/recht/erstes-datenschutzgesetz-in-indien-verabschiedet-1032006; letzter Zugriff am 19.09.2024.

ler personenbezogener Daten dar.[130] Er definiert wesentliche Grundprinzipien, Rechte und Pflichten der betroffenen Personen („Data Principals") sowie die Verantwortlichkeiten der Datenverarbeiter („Data Fiduciaries").[131] Das Gesetz bezieht sich auf die Verarbeitung digitaler personenbezogener Daten in Indien, sofern diese entweder direkt digital erfasst oder nachträglich digitalisiert wurden.[132] Daten, die nicht digitalisiert sind, fallen nicht unter den Anwendungsbereich des DPDP Act.[133] Darüber hinaus gilt das Gesetz extraterritorial, wenn digitale personenbezogene Daten außerhalb Indiens verarbeitet werden, um Waren oder Dienstleistungen für Personen in Indien anzubieten (vgl. Abschnitt 3 lit. b DPDP Act).[134] Die Zentralregierung kann durch entsprechende Verordnungen den Transfer von personenbezogenen Daten in bestimmte ausländische Staaten beschränken (vgl. Sec. 16 DPDP Act, sog. „Negativliste").[135]

Zu den unter den Begriff der Verarbeitung fallenden Tätigkeiten zählen das Sammeln, Aufnehmen, Speichern, Organisieren, Nutzen, Teilen, Löschen oder Zerstören von Daten (vgl. Abschnitt 2 lit. x DPDP Act).[136] Nach Abschnitt 4 darf die Verarbeitung personenbezogener Daten nur in Übereinstimmung mit dem Gesetz sowie für rechtmäßige Zwecke erfolgen, entweder auf Grundlage einer Einwilligung der betroffenen Person (vgl. Abschnitt 6 DPDP Act) oder aufgrund legitimer Nutzungszwecke (vgl. Abschnitt 7 DPDP Act), wie z. B. zur Erfüllung gesetzlicher Verpflichtungen oder in Notfällen im Gesundheitsbereich.[137]

Das Gesetz sieht die Einrichtung des Data Protection Board of India (DPBI) als Aufsichtsbehörde vor (vgl. Kap. V und VI des DPDP Act).[138] Verantwortliche müssen gemäß Sec. 8 des DPDP Act unter anderem angemessene Maßnahmen ergreifen, um Datenschutzverletzungen zu verhindern.[139] Im Falle eines Datenverstoßes müssen sowohl das DPBI als auch die betroffenen Personen informiert werden.[140] Verantwortliche, die eine erhebliche Menge an personenbezogenen Daten verarbeiten, werden als „Significant Data Fiduciaries" eingestuft und unterliegen zusätzlichen Verpflichtungen, wie der Ernennung eines Datenschutzbeauftragten in Indien (vgl. Abschnitt 10 DPDP Act).[141] Auftragsverarbeiter dürfen Daten nur auf der Grundlage eines gültigen Vertrages im Rahmen des Angebots von Waren und Dienstleistungen verarbeiten (vgl. Abschnitt 8 Abs. 2 DPDP Act, „Data Processor").[142]

Bei Verstößen gegen das Gesetz kann das DPBI nach Anhörung der Betroffenen Bußgelder verhängen (vgl. Abschnitt 33 DPDP Act).[143] Die Höhe der Strafen richtet sich nach der Tabelle im Anhang des Gesetzes (Schedule).[144]

Der genaue Zeitpunkt, wann der DPDP Act und seine 44 Bestimmungen in Kraft treten, ist noch nicht bekannt und wird von der Regierung festgelegt.[145] Zusätzlich sind noch detaillierte Durchführungsregelungen für einzelne Bestimmungen zu erwarten (vgl. Abschnitt 40 DPDP Act).[146]

Mit der Einführung des DPDP Act wird das Gesetz die bisherigen Datenschutzregelungen, darunter den Information Technology Act, 2000 (insbesondere Abschnitt 43A) sowie die Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, ablösen.[147]

3. Angemessenheitsbeschluss

Derzeit gibt es keinen Angemessenheitsbeschluss der Europäischen Union für Indien. Das bedeutet, dass Unternehmen, die personenbezogene Daten von der EU nach Indien übermitteln möchten, alternative Mechanismen verwenden müssen, um die Anforderungen der DSGVO zu erfüllen. Es bleibt abzuwarten, wie sich die

130 https://www.gtai.de/de/trade/indien/recht/erstes-datenschutzgesetz-in-indien-verabschiedet-1032006; letzter Zugriff am 19.09.2024.
131 https://www.gtai.de/de/trade/indien/recht/erstes-datenschutzgesetz-in-indien-verabschiedet-1032006; letzter Zugriff am 19.09.2024.
132 https://www.gtai.de/de/trade/indien/recht/erstes-datenschutzgesetz-in-indien-verabschiedet-1032006; letzter Zugriff am 19.09.2024.
133 https://www.gtai.de/de/trade/indien/recht/erstes-datenschutzgesetz-in-indien-verabschiedet-1032006; letzter Zugriff am 19.09.2024.
134 https://www.gtai.de/de/trade/indien/recht/erstes-datenschutzgesetz-in-indien-verabschiedet-1032006; letzter Zugriff am 19.09.2024.
135 https://www.gtai.de/de/trade/indien/recht/erstes-datenschutzgesetz-in-indien-verabschiedet-1032006; letzter Zugriff am 19.09.2024.
136 https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf; letzter Zugriff am 19.09.2024.
137 https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf; letzter Zugriff am 19.09.2024.
138 https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf; letzter Zugriff am 19.09.2024.
139 https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf; letzter Zugriff am 19.09.2024.
140 https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf; letzter Zugriff am 19.09.2024.
141 https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf; letzter Zugriff am 19.09.2024.
142 https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf; letzter Zugriff am 19.09.2024.
143 https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf; letzter Zugriff am 19.09.2024.
144 https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf; letzter Zugriff am 19.09.2024.
145 https://www.gtai.de/de/trade/indien/recht/erstes-datenschutzgesetz-in-indien-verabschiedet-1032006; letzter Zugriff am 19.09.2024.
146 https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf; letzter Zugriff am 19.09.2024.
147 https://www.gtai.de/de/trade/indien/recht/erstes-datenschutzgesetz-in-indien-verabschiedet-1032006; letzter Zugriff am 19.09.2024.

aktuellen Gesetzesinitiativen hierauf auswirken werden.

III. Zwischenfazit Indien

Der aktuelle Stand des indischen Datenschutzes zeigt, dass Indien erhebliche Fortschritte auf dem Weg zu einer umfassenden Datenschutzgesetzgebung gemacht hat. Obwohl frühere Versuche, ein solches Gesetz zu verabschieden, gescheitert sind, hat sich mit der Verabschiedung des DPDP Act 2023 ein wichtiger Durchbruch ergeben. Dieses Gesetz bildet den ersten eigenständigen Rechtsrahmen für den Schutz digitaler personenbezogener Daten in Indien und orientiert sich an internationalen Standards wie der DSGVO. Es regelt den Umgang mit digitalen Daten, führt Aufsichtsbehörden ein und setzt strenge Vorgaben für Unternehmen, um den Datenschutz zu gewährleisten. Jedoch bleibt abzuwarten, wie die Umsetzung erfolgt und welche Auswirkungen das Gesetz international, insbesondere auf die Datenübertragung zwischen der EU und Indien, haben wird.

E. Vergleich und Analyse

I. Vergleich von Südkoreas, Chinas und Indiens Position im asiatischen Datenschutz-Kontext

Insgesamt zeigen alle drei Rechtsordnungen im Bereich des Datenschutzes deutliche Parallelen zur DSGVO. Dabei nimmt Südkorea eine klare Vorreiterposition ein. Zudem stellt das südkoreanische Datenschutzrecht nicht nur im Vergleich mit den anderen asiatischen Rechtsordnungen, sondern auch im Vergleich mit der DSGVO teilweise strengere Anforderungen.

Auch Chinas Datenschutzrecht zeigt einige Ähnlichkeiten zur DSGVO und zu den anderen asiatischen Rechtsordnungen. Allerdings treten im chinesischen Datenschutzrecht, anders als etwa im südkoreanischen Datenschutzrecht, auch klare politische Motive in den Vordergrund. Chinas Staatsstrukturen sind geprägt von Kontrolle und Überwachung. Ein Datenschutzrecht, das an ein Datenschutzgrundrecht anknüpft, würde insofern die Ziele des chinesischen Staats verfehlen. Deshalb zeigen sich im PIPL deutliche Unterschiede zwischen den Vorgaben für private Unternehmen und staatliche Einrichtungen.

Indien liegt hingegen im Vergleich zu Südkorea und China auf Ebene des Datenschutzes deutlich zurück. Auch wenn mittlerweile ein Datenschutzgesetz verabschiedet wurde, ist dies bis zum heutigen Zeitpunkt weder in Kraft noch wurde hierfür ein Termin bestimmt. Insgesamt weist aber zumindest auch das geplante indische Datenschutzgesetz positiv zu bewertende Strukturen auf, die den Datenschutz in Indien stark verbessern könnten.

II. Auswirkungen auf internationale Unternehmen

Für international agierende Unternehmen kann die uneinheitliche globale Datenschutzlandschaft eine enorme Herausforderung darstellen. Gerade im Bereich des Datenverkehrs ist dies ein Problem, da dieser auch von internationalem Transfer lebt und insbesondere durch ihn die Globalisierung auch ihre positiven Effekte entfalten kann.

Erfreulich ist zumindest, dass ein Großteil der Regeln ähnliche Strukturen zu denen der DSGVO aufweist. Das erleichtert global agierenden Stellen nicht nur die Verständlichkeit der einzelnen Vorgaben, sondern ermöglicht auch eine einfachere und effektivere Umsetzung der verschiedenen Vorgaben. Da die DSGVO bereits sehr hohe Standards setzt, müssen EU-Unternehmen insofern nur bezüglich einzelner spezieller Regelungen ihre Datenschutzpraktiken anpassen. Nichtsdestotrotz ist enorme Vorsicht geboten, denn, wie zuvor aufgezeigt, hat insbesondere Südkorea an verschiedenen Stellen deutlich strengere Regeln als die DSGVO. Andererseits können sich Unternehmen dann aufgrund des Vorliegens eines Angemessenheitsbeschlusses bei solchen Geschäftsbeziehungen eher auf die Sicherheit der Datenübertragungen verlassen.

Eine Herausforderung stellt zudem im Datenverkehr mit asiatischen Staaten auch der Trend zur Datenlokalisierung und zur extraterritorialen Wirkung dar. Sowohl China als auch in Zukunft Indien verlangen eine lokale Speicherung von Daten. Daneben müssen sich Unternehmen bei Beziehungen zu Staaten, die eine grenzüberschreitende Wirkung bestimmt haben, mit den nationalen Datenschutzgesetzen auseinandersetzen, auch wenn sie keinen Sitz im jeweiligen Land haben. Das kann im Einzelfall einen enormen bürokratischen Aufwand bedeuten.

F. Schlussfolgerung

Zusammenfassend lässt sich feststellen, dass China, Südkorea und Indien zunehmend anspruchsvolle Datenschutzregelungen entwickelt haben, die in vielerlei Hinsicht mit den globalen Standards konkurrieren. Chinas umfassendes System, bestehend aus dem PIPL und dem DSL, setzt strenge Anforderungen für Datenverarbeitung und Datensicherheit, während Südkorea mit seinem PIPA eines der fortschrittlichsten Daten-

schutzgesetze in Asien hat. Indien, das mit dem DPDP 2023 erstmals ein eigenständiges Datenschutzgesetz verabschiedet hat, stärkt seine Position im globalen Datenschutzdiskurs.

Asien spielt folgerichtig eine zunehmend bedeutende Rolle in der internationalen Datenschutzlandschaft. Diese Länder setzen nicht nur regionale Maßstäbe, sondern prägen auch den weltweiten Datenschutzrahmen, insbesondere durch ihre extraterritorialen Bestimmungen und die wachsende digitale Wirtschaft. Asien ist nicht nur eine der am schnellsten wachsenden Wirtschaftsregionen der Welt, sondern auch ein bedeutender Knotenpunkt für technologische Innovationen und digitale Dienstleistungen. Länder wie China, Südkorea und Indien spielen eine Schlüsselrolle in der globalen Wirtschaft, insbesondere in den Bereichen E-Commerce, Künstliche Intelligenz und Finanztechnologie. Mit dieser wirtschaftlichen Dynamik wächst auch die Menge an personenbezogenen Daten, die gesammelt, verarbeitet und gespeichert werden – was den Datenschutz zu einem zentralen Thema für Unternehmen und Regierungen macht.

Der Datenschutz ist in Asien daher nicht nur eine Frage der gesetzlichen Compliance, sondern auch ein entscheidender Wettbewerbsfaktor. Unternehmen, die in der Region agieren, müssen sicherstellen, dass sie den wachsenden Anforderungen an den Schutz personenbezogener Daten gerecht werden, um Vertrauen bei Verbrauchern und Geschäftspartnern zu schaffen. Gleichzeitig ermöglicht ein robustes Datenschutzregime, internationale Kooperationen zu stärken und ausländische Investitionen zu fördern. Asiens wirtschaftliche Relevanz im globalen Markt wird also zunehmend mit den strengen und weitreichenden Datenschutzgesetzen verknüpft, was die Region zu einem Vorreiter im globalen Datenschutzdiskurs macht.

Unternehmen, die in diesen Märkten tätig sind oder Daten von asiatischen Nutzern verarbeiten, sollten sicherstellen, dass sie die unterschiedlichen Regelungen einhalten. Gleichzeitig sind politische Entscheidungsträger gefordert, kontinuierlich an der Harmonisierung der Datenschutzstandards zu arbeiten, um die grenzüberschreitende Datenverarbeitung effizienter und sicherer zu gestalten. Zusammenarbeit und Dialog auf globaler Ebene sind dabei unerlässlich, um den Datenschutz weltweit zu stärken und gleichzeitig die Innovationskraft der digitalen Wirtschaft zu fördern.

Rechtsanwalt **Dr. Kinast** ist Gründer und geschäftsführender Gesellschafter von KINAST Rechtsanwälte. Er ist externer Datenschutzbeauftragter zahlreicher nationaler und internationaler Großkonzerne, Banken und Versicherungen sowie Organisationen der Kirche und öffentlichen Hand. Weiterhin berät Herr Dr. Kinast als externer Compliancebeauftragter diverse Unternehmen der verschiedensten Branchen.