Personal Information Protection Law

www.datenschutzsysteme.com

1. Das PIPL und sein Verhältnis zur DSGVO

Das PIPL ist die chinesische Antwort auf die europäische DSGVO. Wie auch in der EU, sollen chinesischen Staatsbürger:innen Sicherheitsgarantien geboten werden, dass ihre personenbezogene Daten (pbD) nicht missbraucht, ohne ihr Wissen verkauft und vor allem sicher verarbeitet werden. Es gibt viele Parallelen der beiden Regularien. Das Verständnis davon, was als personenbezogene Daten gilt (im PIPL wird von persönlichen Daten gesprochen) ist sehr ähnlich. Beide betrachten Daten, die eine Person identifizieren oder identifizierbar machen als pbD; beide schaffen die Möglichkeit diese Daten zu anonymisieren und beide haben ein ziemlich deckungsgleiches Verständnis des Begriffs der Datenverarbeitung (Artikel 4 PIPL, übersetzt von Webster, 2022).

Eine wichtige Unterscheidung in der Begrifflichkeit ist das Konzept des "Verantwortlichen" (eng. "controller"). Diese juristische oder natürliche Person ist in der DGVO die, die über die Zwecke und Mittel der Verarbeitung entscheidet und als "Besitzer" der Daten gilt. Im PIPL heißt diese Rolle "Verarbeiter persönlicher Daten" (Recha & Burkardt, 2022). Als Verarbeiter gelten in der DSGVO allerdings alle Beteiligten, die an einer Datenverarbeitung beteiligt sind, mit Ausnahme der betroffenen Person. Das kann zu Verwirrung führen.

Die **Rechtsgrundlagen** für eine Verarbeitung sind sowohl in der DSVGVO als auch im PIPL klar definiert (Art. 6 DSGVO; § 13 PIPL). Der einzige wesentliche Unterschied ist die Grundlage des berechtigen Interesses (Art. 6 I f) DSGVO). Das existiert im PIPL nicht. Firmen, die sowohl in der EU und in China operieren, müssen hier besonders aufpassen und die Datenerhebung entsprechend anpassen (Recha & Burkardt, 2022). Eine weitere Besonderheit in den Rechtsgrundlagen ist die Bedeutung von Einwilligungen. Während in der DSGVO eine Einwilligung einmalig eingeholt werden muss, um die Daten z.B. ins Ausland zu übermitteln, muss gem. des PIPLs bei jedem neuen Grenzübertritt eine erneute Einwilligung für dieses bestimmte Land erfragt werden. Hierauf wird später noch einmal eingegangen.

Die **betroffenen Rechte** der DSGVO und des PIPLs sind so gut wie deckungsgleich. Es gibt feine Unterschiede, aber sowohl in Bezeichnung als auch Sinn und Zweck der Rechte, ähneln sich beide Datenschutzgesetze sehr stark.

Was als **besonders schützenswerte Kategorien der Daten** gilt, geht in den beiden Texten auseinander. Dem PIPL fehlen die Kategorien der: "politischen Meinung", "ethnische Herkunft", "Gewerkschaftszugehörigkeit" und "sexuelle Orientierung".

Überblick zum PIPL

Im November 2021 trat das Gesetz zum Schutz personenbezogener Daten (GSPD) oder **P**ersonal **I**nformation **P**rotection **L**aw (PIPL) in der Volksrepublik China in Kraft.

Das Gesetz wird häufig als die DSGVO Chinas bezeichnet (weber.digital, 2022). Es stellt den ersten Versuch der Volksrepublik dar, umfassende Regularien zu erstellen, die den Schutz von personenbezogenen Daten der eigenen Bürger:innen innerhalb der Landesgrenzen, aber auch darüber hinaus sicherstellen.

Für Unternehmen, die aus der Europäischen Union heraus mit Partner:innen in China zusammenarbeiten kann das PIPL unter Umständen zu Herausforderungen führen. Dieser Report soll eine Übersicht darüber geben, was das PIPL ist, wer unter seinen Anwendungsbereich fällt und welche Herausforderungen auf Unternehmen im Anwendungsbereich der DSGVO zukommen können.

Außerdem wird eine Übersicht gegeben, wie diesen Herausforderungen beizukommen ist und welche Risiken, Vor- und Nachteile dadurch entstehen können

Dafür fügt des PIPL auch einige Kategorien hinzu. Neben "Daten über den Aufenthaltsort", "persönliche Daten von Minderjährigen unter 14 Jahren", "Finanzkonten" und der sehr breiten Kategorie von "anderen persönlichen Daten", fallen auch "bestimmte Identitäten" unter die besonders zu schützenden Daten. Insbesondere letzteres wird eher selten für Firmen der Fall sein (Recha & Burkardt, 2022).

Das Verarbeiten solcher Daten, ist im PIPL nur mit Erfüllung sehr strenger Schutz-Anforderungen erlaubt.

1.1. Separate Einwilligung

Das PIPL verlangt eigenständige Einwilligungen, wenn eine chinesische Firma persönliche Daten an Dritte bereitstellt, Daten veröffentlicht werden, Daten aus den besonderen Kategorien verarbeitet werden und bei jeder Grenzüberschreitung von persönlichen Daten (Art. 39 PIPL, übersetzt von Webster, 2022).

Letzteres ist insbesondere wichtig für die Arbeitsabläufe in Firmen. Auch wenn eine europäische Firma persönliche Daten von chinesischen Staatsbürger:innen, von Deutschland nach Österreich übermittelt, muss eine separate Einwilligung dieser Menschen eingeholt werden. Es wird also nötig werden, eng mit den chinesischen Partner:innen oder Tochterfirmen zusammenzuarbeiten, um dem PIPL gerecht zu werden.

2. Datenübermittlung über Grenzen

Ist man mit den grenzübergreifenden Datenübermittlungen in der DSGVO vertraut, muss man für das PIPL etwas umdenken. Zunächst existiert kein gleichwertiges Mittel zu "adequacy decisions" der Kommission (Securiti Research Team, 2022). Das heißt, das zu diesem Zeitpunkt kein Land existiert, in das chinesische Firmen bedenkenlos Daten übermitteln können. Allerdings hält das PIPL die Möglichkeit offen, die Datenschutzgesetze anderer Länder in gegenseitigem Einverständnis anzuerkennen. Für die EU bedeutet das, dass die Kommission das PIPL als "adequate" einstufen müsste, damit die Chinesische Regierung die DSGVO als bedenkenlos einstuft. Ob und wann das passiert, bleibt abzuwarten.

Für Grenzüberschreitungen bietet das PIPL allerdings company to company Lösungen, die unabhängig von nationalen Bestimmungen den Datentransfer ermöglichen können.

Zunächst muss eine separate Einwilligung der betroffenen Person eingeholt werden. Dieser Schritt ist kategorisch notwendig, sobald pbD das Land wechseln. Die chinesische Firma (oder alternativ die Tochtergesellschaft in China) ist außerdem dafür verantwortlich, dass im Zielland ein angemessener Datenschutzstandard herrscht (Recha & Burkardt, 2022). Zusätzlich dazu ist eine Datenschutzfolgeabschätzung (DSFA) unbedingt notwendig (Chen, 2022), die sich in einigen Bereichen von einer europäischen DSFA unterscheidet.

Nachdem alle diese Schritte erfolgt sind, können sog. "Übermittlungsinstrumente" (Art. 38 PIPL) zum Einsatz kommen.

2.1. Übermittlungsinstrumente

Als solche Übermittlungsinstrumente gelten: Sicherheitsaudits, Zertifikate und chinesische Standardverträge (Chen, 2022; Recha & Burkardt, 2022).

Sicherheitsaudits sind ein Mittel, das die "Cyberspace Administration of China" (CAC) als notwendig erachtet, wenn gewisse Kriterien erfüllt sind. Werden:

- "wichtige Daten" (definiert im Datensicherheitsgesetz),
- Daten in der "kritischen Informationsinfrastruktur" (Cybersicherheitsgesetz),
- Daten von mehr als 1 Mio. Menschen ohne zeitliche Begrenzung,
- im letzten Kalenderjahr Daten von mehr als 100.000 oder
- im letzten Kalenderjahr sensible Daten von mehr als 10.000 Menschen

verarbeitet, so sieht die CAC ein Sicherheitsaudit als unbedingt notwendig. Ohne ein bestandenes Audit wird eine Übermittlung ins Ausland nicht gestattet. Zunächst müssen die Firmen eine Selbstprüfung durchführen. Diese Selbstprüfung und zusätzliche Vertragsdokumente müssen dann bei der lokalen CAC Behörde eingereicht werden. Nach eingehender Prüfung leitet das CAC dann das tatsächliche Sicherheitsaudit ein. Ein bestandenes Audit ist für zwei Jahre gültig. (weber.digital, 2022)

Datenschutz Zertifizierungen sind eine Möglichkeit für Unternehmen, die keinen Sitz in China haben, den allgemeinen Transfer zu erleichtern. Voraussetzung dafür ist, dass kein Audit notwendig ist. Die Anforderungen an das Unternehmen sind hoch. Es muss ein Vertrag zwischen beiden Parteien bestehen, ein:e DSB muss festgelegt werden und eine Datenschutzfolgeabschätzung muss durchgeführt sein. Erst danach kann eine Zertifizierungsantrag gestellt werden. Eingereicht werden muss:

- Eine Firmenlizenz bzw. ein Firmennachweis beider Parteien
- Der oben genannte Vertrag zwischen beiden Parteien sowie die Datenschutz-Folgeabschätzung
- Ein Organigramm beider Parteien, welches die Funktion aller Abteilungen beschreibt
- Ein ausgefülltes Formular zur Selbsteinschätzung, welches jedoch noch nicht näher spezifiziert ist
- Eine Erklärung des geplanten Datentransfers sowie die Art und Kategorisierung der Daten
- Einen Nachweis, dass keine der beiden Parteien in den letzten 12 Monaten ein Datenleck hatte

Eine solche Zertifizierung ist für drei Jahre gültig. (weber.digital, 2022)

Der **Standardvertrag** ist das go-to Mittel für grenzüberschreitende Datenübermittlung. Er ist nur anwendbar, wenn kein Audit notwendig ist (also keines der oben genannten Kriterien greift). Ähnlich einem AVV oder den EU-SCCs, definiert dieser Vertrag Rechte und Pflichten der beiden Vertragsparteien, Kontaktmöglichkeiten, etc. Allerdings ist die chinesische Variante in einigen Bereichen strenger, als es die EU Regeln sind. Zunächst müssen Daten sobald die Verarbeitung endet unmittelbar gelöscht werden. Wichtiger ist allerdings, dass die CAC die Aufsicht auch für ausländische Firmen übernimmt, auf Anfrage alle relevanten Informationen der CAC gegenüber offengelegt werden müssen und mögliche Rechtsstreite in Zusammenhang mit dem Vertrag in China selbst ausgetragen werden müssen (Chen, 2022; Roberts et al., 2023; weber.digital, 2022).

Zusätzlich muss mit jedem Standardvertrag eine DSFA angefertigt werden. Dazu gehört z.B. auch Firmeninterne Prozesse, die mit der Datenübermittlung zu tun haben, offenzulegen, aber auch eine Einschätzung der rechtlichen Rahmenbedingungen zum Datenschutz in den - aus der Perspektive Chinas - Drittländern. Es empfiehlt sich also bei jedem Datentransfer mit China, rechtlichen Beistand zumindest zu konsultieren.

Für einen ausführlichen Vergleich siehe auch: Roberts et al. (2023).

3. Abschluss

Aus Sicht der betroffenen Personen stellt das PIPL eine bahnbrechende Entwicklung dar. Es ist das erste Gesetz außerhalb der DSGVO, dass Datenschutz wirklich ernst nimmt. Allerdings schwingen mit dem PIPL gewisse Randbedingungen mit. Ähnlich der Entwicklung der DSGVO zielt auch das PIPL in seinen Kinderschuhen auf das Schützen nationaler Interessen ab. Es ist auch wichtig im Hinterkopf zu behalten, dass selbst in der EU das Thema Datenschutz noch immer im Wandel ist und in rascher Abfolge immer wieder neue Regelungen entstehen. Etwas derartiges kann auch von dem chinesischen Gesetz erwartet werden.

Selbst für Datenschutz-affine europäische Unternehmen bedeutet das PIPL aktuell noch viel Arbeit. Nicht zuletzt könnte eine Anpassung der Datenschutzerklärung für den chinesischen Raum anstehen und je nach Art der Datenverarbeitungen sogar die Berufung einer:s eigenen chinesischen Datenschutzbeauftragten.

Auch die Aufsicht der CAC ist etwas mit der sich europäische Firmen noch vertraut machen müssen. Die Datenschuttaufsichtsbehörden in der EU sind je nach Land relativ "hands-off" und greifen nur ein, wenn es offensichtliche Verstöße gibt. Von der CAC kann mehr Intervention erwartet werden, insbesondere im Hinblick auf die Sicherheitsaudits für kritische Infrastruktur und "wichtige Daten".

All das sollte aber nicht für schlaflose Nächte sorgen. Neue Gesetze brauchen immer etwas Zeit, um sich "zu finden". Als die DSGVO eingeführt wurde, gab es z.B. die Debatte, ob Namen auf Klingelschildern noch erlaubt sind oder nicht. Auch die Behörden müssen sich erst mit dem Gesetz zurechtfinden. In Einzelfällen wird es sicherlich Fehlentscheidungen geben und manche Behörden und Firmen werden auch mit Kanonen auf Spatzen schießen. Insgesamt muss sich das Gesetz erst entwickeln und die gängige Praxis sich einstellen.

Zusätzlich sollte man immer auch einen Blick für die internationalen Beziehungen zwischen der EU und China haben. Die chinesische Regierung hat bereits signalisiert, dass sie die DSGVO als gleichwertig zum PIPL anerkennen wird, wenn die Kommission das auch tut. Zum aktuellen Zeitpunkt (Juli 2023) ist das noch relativ unwahrscheinlich, aber auf lange Sicht gesehen, kann es hier zu interessanten Entwicklungen kommen.

Es bleibt allerdings bestehen, dass jede Firmen die mit Datentransfers aus China heraus zu tun hat, sich im Zweifel mit Kanzleien mit Expertise im dem Bereich auseinandersetzt und mit den chinesischen Partern:innen vor Ort eng zusammenarbeitet, um Geldstrafen und rechtliche Konsequenzen zu vermeiden.

Bibliografie

Chen, A. (2022, September 5). *Internationaler Datentransfer: Die neuen chinesischen SCC (Entwurf)*. Dr. Datenschutz. https://www.dr-datenschutz.de/internationaler-datentransfer-die-neuen-chinesischen-scc-entwurf/

Chinas neues Datensicherheitsgesetz. (2021, August 6). *datenschutzticker.de*. https://www.datenschutzticker.de/2021/08/chinas-neues-datensicherheitsgesetz/

Czarnocki, Giglio, Kun, Petik, & Royer. (2021). *Government access to data in third countries Final Report* (Report EDPS/2019/02-13). https://edpb.europa.eu/our-work-tools/our-documents/legal-study-external-provider/legal-study-government-access-data-third_en

Recha, J., & Burkardt, R. (2022). *Das neue chinesische Datenschutzrecht und die europäische DSGVO im Rechtsvergleich—Burkardt & Partner*. https://www.bktlegal.com/news-events/das-neue-chinesische-datenschutzrecht-und-die-europaeische-dsgvo-im-rechtsvergleich.html

Roberts, A., Li, R., & Ke, T. (2023, March 7). *China's standard contract for cross-border data transfers released: Key implications and comparison against the EU SCCs*. Www.Linklaters.Com. https://www.linklaters.com/en/insights/blogs/digilinks/2023/march/chinas-standard-contract-for-cross-border-data-transfers-released

Securiti Research Team. (2022, July 7). *Understanding Cross Borders Data Transfers Under GDPR and PIPL*. Securiti. https://securiti.ai/blog/cross-borders-data-transfers-pipl/

weber.digital. (2022). *Chinas DSGVO: Schutz von personenbezogenen Daten in China (GSPD)*. https://service.weber.digital/index.php?/Knowledgebase/Article/View/chinas-dsgvo-schutz-von-personenbezogenen-daten-in-china

Webster, R. (2022). Translation: Personal Information Protection Law of the People's Republic of China - Effective Nov. 1, 2021. *DigiChina*. https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

OPTIQUM GmbH
Siegburger Straße 223
D-50679 Köln

+49 221 82 95 91 0
info@optiqum.de