

Übersetzung

Gesetz zum Schutz personenbezogener Daten der Volksrepublik China (Inkrafttreten zum 01.11.2021)

(Personal Information Protection Law of the People's Republic of China (Effective Nov. 1, 2021))

HINWEIS: Diese Übersetzung (Stand 2021-08-28) basiert auf der ins Englische übersetzten Fassung des chinesischen Gesetzes von Rogier Creemers und Graham Webster auf der Grundlage der früheren Übersetzung des zweiten Entwurfs des Gesetzes durch DigiChina, die wiederum auf der Übersetzung des ersten Entwurfs von Rogier Creemers, Mingli Shi, Lauren Dudley und Graham Webster basiert.

Quelle: <https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021>

Diese Übersetzung soll einen leichten Überblick über das chinesische Datenschutzgesetz in deutscher Sprache geben. Sie erhebt jedoch keinesfalls Anspruch auf Richtigkeit.

Gesetz zum Schutz personenbezogener Daten der Volksrepublik China (Inkrafttreten zum 01.11.2021)

- Kapitel I:** Allgemeine Bestimmungen
- Kapitel II:** Regeln für den Umgang mit personenbezogenen Daten
 - Abschnitt 1:** Gewöhnliche Bestimmungen
 - Abschnitt 2:** Vorschriften für den Umgang mit sensiblen personenbezogenen Daten
 - Abschnitt 3:** Besondere Bestimmungen für den Umgang mit personenbezogenen Daten durch staatliche Behörden
- Kapitel III:** Vorschriften über die grenzüberschreitende Übermittlung personenbezogener Daten
- Kapitel IV:** Rechte des Einzelnen bei der Verarbeitung personenbezogener Daten
- Kapitel V:** Pflichten der Bearbeiter personenbezogener Informationen
- Kapitel VI:** Dienststellen, die die Pflichten und Verantwortlichkeiten im Bereich des Schutzes personenbezogener Daten wahrnehmen
- Kapitel VII:** Gesetzliche Haftung
- Kapitel VIII:** Ergänzende Bestimmungen

Kapitel I: Allgemeine Bestimmungen

Artikel 1: Dieses Gesetz wurde auf der Grundlage der Verfassung formuliert, um die Rechte und Interessen von Personen zu schützen, den Umgang mit personenbezogenen Daten zu vereinheitlichen und die rationelle Nutzung von personenbezogenen Daten zu fördern.

Artikel 2: Die persönlichen Daten natürlicher Personen werden rechtlich geschützt; keine Organisation oder Einzelperson darf die Rechte und Interessen natürlicher Personen in Bezug auf persönliche Daten verletzen.

Artikel 3: Dieses Gesetz gilt für den Umgang mit persönlichen Daten natürlicher Personen innerhalb der Grenzen der Volksrepublik China.

Wenn einer der folgenden Umstände bei der Verarbeitung personenbezogener Daten natürlicher Personen innerhalb der Grenzen der Volksrepublik China außerhalb der Grenzen der Volksrepublik China gegeben ist, gilt dieses Gesetz ebenfalls:

1. wenn der Zweck darin besteht, Produkte oder Dienstleistungen für natürliche Personen innerhalb der Grenzen bereitzustellen;
2. bei der Analyse oder Bewertung von Aktivitäten natürlicher Personen innerhalb der Grenzen;
3. unter sonstigen in Gesetzen oder Verwaltungsvorschriften vorgesehenen Voraussetzungen.

Artikel 4: Personenbezogene Daten sind alle Arten von Daten, die mit elektronischen oder anderen Mitteln aufgezeichnet werden und sich auf identifizierte oder identifizierbare natürliche Personen beziehen, mit Ausnahme von Daten nach Anonymisierung.

Der Umgang mit personenbezogenen Daten umfasst die Erhebung, Speicherung, Verwendung, Verarbeitung, Übermittlung, Bereitstellung, Weitergabe, Löschung usw.

Artikel 5: Bei der Verarbeitung personenbezogener Daten sind die Grundsätze der Rechtmäßigkeit, Angemessenheit, Notwendigkeit und Aufrichtigkeit zu beachten. Es ist verboten, personenbezogene Daten auf irreführende, betrügerische, erzwungene oder sonstige Weise zu verarbeiten.

Artikel 6: Die Verarbeitung personenbezogener Daten muss einen klaren und angemessenen Zweck haben und direkt mit dem Verarbeitungszweck verbunden sein, wobei eine Methode mit dem geringsten Einfluss auf die Rechte und Interessen des Einzelnen anzuwenden ist.

Die Sammlung personenbezogener Daten ist auf den kleinstmöglichen Umfang zu beschränken, um den Verarbeitungszweck zu erreichen, und eine übermäßige Sammlung personenbezogener Daten ist verboten.

Artikel 7: Bei der Verarbeitung personenbezogener Daten sind die Grundsätze der Offenheit und Transparenz zu beachten, indem die Regeln für die Verarbeitung personenbezogener Daten offengelegt und Zweck, Methode und Umfang der Verarbeitung klar angegeben werden.

Artikel 8: Bei der Verarbeitung personenbezogener Daten ist die Qualität der personenbezogenen Daten zu gewährleisten und eine Beeinträchtigung der Rechte und Interessen des Einzelnen durch ungenaue oder unvollständige personenbezogene Daten zu vermeiden.

Artikel 9: Die Verantwortlichen für den Umgang mit personenbezogenen Daten tragen die Verantwortung für ihre Tätigkeiten im Umgang mit personenbezogenen Daten und ergreifen die erforderlichen Maßnahmen, um die Sicherheit der von ihnen verarbeiteten personenbezogenen Daten zu gewährleisten.

Artikel 10: Keine Organisation oder Einzelperson darf personenbezogene Daten anderer Personen unrechtmäßig sammeln, verwenden, verarbeiten oder übermitteln oder personenbezogene Daten anderer Personen unrechtmäßig verkaufen, kaufen, zur Verfügung stellen oder weitergeben oder sich an Tätigkeiten zur Verarbeitung personenbezogener Daten beteiligen, die der nationalen Sicherheit oder dem öffentlichen Interesse schaden.

Artikel 11: Der Staat richtet eine Struktur zum Schutz persönlicher Informationen ein, um Handlungen zu verhindern und zu bestrafen, die die Rechte auf und Interessen an persönlichen Informationen verletzen, um die Werbung für den Schutz persönlicher Informationen und die Aufklärung zu verstärken und um die Schaffung eines guten Umfelds für den Schutz persönlicher Informationen zu fördern, unter gemeinsamer Beteiligung von Regierung, Unternehmen, relevanten gesellschaftlichen Organisationen und der allgemeinen Öffentlichkeit.

Artikel 12: Der Staat beteiligt sich nachdrücklich an der Ausarbeitung internationaler Regeln [oder Normen] für den Schutz persönlicher Daten, fördert den internationalen Austausch und die Zusammenarbeit im Bereich des Schutzes persönlicher Daten und unterstützt die gegenseitige Anerkennung von Regeln [oder Normen], Standards usw. zum Schutz persönlicher Daten mit anderen Ländern, Regionen und internationalen Organisationen.

Kapitel II: Vorschriften für den Umgang mit personenbezogenen Daten

Abschnitt 1: Gewöhnliche Bestimmungen

Artikel 13: Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn eine der folgenden Bedingungen erfüllt ist:

1. Einholung der Zustimmung der Person;
2. Wenn es notwendig ist, um einen Vertrag abzuschließen oder zu erfüllen, an dem die Person eine interessierte Beteiligte ist, oder wenn es notwendig ist, um die Personalverwaltung in Übereinstimmung mit rechtmäßig formulierten Arbeitsregeln und -strukturen und rechtmäßig geschlossenen Verträgen durchzuführen;
3. wenn dies zur Erfüllung gesetzlicher Aufgaben und Zuständigkeiten oder gesetzlicher Verpflichtungen erforderlich ist;

4. wenn es erforderlich ist, um auf plötzliche Zwischenfälle im Bereich der öffentlichen Gesundheit zu reagieren oder das Leben und die Gesundheit natürlicher Personen oder die Sicherheit ihres Eigentums in Notfällen zu schützen;
5. Verarbeitung personenbezogener Daten in einem angemessenen Umfang zur Durchführung von Nachrichtenberichterstattung, Überwachung der öffentlichen Meinung und anderen Aktivitäten im öffentlichen Interesse;
6. Bei der Verarbeitung personenbezogener Daten, die von Personen selbst offengelegt wurden oder auf andere Weise bereits rechtmäßig offengelegt wurden, in einem angemessenen Umfang in Übereinstimmung mit den Bestimmungen dieses Gesetzes.
7. Andere in Gesetzen und Verwaltungsvorschriften vorgesehene Umstände.
8. In Übereinstimmung mit anderen einschlägigen Bestimmungen dieses Gesetzes ist beim Umgang mit personenbezogenen Daten die Zustimmung des Einzelnen einzuholen. Die Einholung der Zustimmung des Einzelnen ist jedoch unter den Bedingungen der Punkte 2 bis 7 nicht erforderlich.

Artikel 14: Wenn personenbezogene Daten auf der Grundlage einer individuellen Einwilligung verarbeitet werden, muss diese Einwilligung von den Betroffenen in voller Kenntnis der Sachlage und in einer freiwilligen und ausdrücklichen Erklärung erteilt werden. Soweit Gesetze oder Verwaltungsvorschriften vorsehen, dass für die Verarbeitung personenbezogener Daten eine gesonderte Einwilligung oder eine schriftliche Zustimmung einzuholen ist, sind diese Bestimmungen zu befolgen.

Ändert sich der Zweck der Verarbeitung personenbezogener Daten, die Verarbeitungsmethode oder die Kategorien der verarbeiteten personenbezogenen Daten, so ist die Zustimmung des Betroffenen erneut einzuholen.

Artikel 15: Werden personenbezogene Daten auf der Grundlage einer individuellen Einwilligung verarbeitet, hat der Einzelne das Recht, seine Einwilligung zu widerrufen. Die für die Verarbeitung personenbezogener Daten Verantwortlichen müssen eine bequeme Möglichkeit zum Widerruf der Einwilligung anbieten.

Wenn eine Person ihre Einwilligung widerruft, hat dies keine Auswirkungen auf die Wirksamkeit der Verarbeitung personenbezogener Daten, die auf der Grundlage der Einwilligung der Person vor dem Widerruf erfolgt ist.

Artikel 16: Die für die Verarbeitung personenbezogener Daten Verantwortlichen dürfen die Bereitstellung von Produkten oder Dienstleistungen nicht mit der Begründung verweigern, dass eine Person der Verarbeitung ihrer personenbezogenen Daten nicht zustimmt oder ihre Zustimmung widerruft, es sei denn, die Verarbeitung personenbezogener Daten ist für die Bereitstellung von Produkten oder Dienstleistungen erforderlich.

Artikel 17: Die für die Verarbeitung personenbezogener Daten Verantwortlichen müssen die Personen vor der Verarbeitung personenbezogener Daten ausdrücklich wahrheitsgemäß, genau und vollständig über die folgenden Punkte in einer klaren und leicht verständlichen Sprache informieren:

1. Den Namen oder den persönlichen Namen und die Kontaktmöglichkeit des Bearbeiters personenbezogener Daten;
2. den Zweck der Verarbeitung personenbezogener Daten und die Verarbeitungsmethoden, die Kategorien der verarbeiteten personenbezogenen Daten und die Aufbewahrungsfrist;
3. Methoden und Verfahren für Einzelpersonen zur Ausübung der in diesem Gesetz vorgesehenen Rechte;
4. Andere Punkte, die in Gesetzen oder Verwaltungsvorschriften vorgesehen sind, müssen mitgeteilt werden.
5. Tritt eine Änderung der im vorigen Absatz genannten Punkte ein, so sind die Betroffenen über die Änderung zu informieren.

Wenn die für die Verarbeitung personenbezogener Daten Verantwortlichen die in Absatz 1 genannten Angelegenheiten durch die Formulierung von Regeln für die Verarbeitung personenbezogener Daten bekannt geben, werden die Regeln für die Verarbeitung öffentlich gemacht [bekannt gegeben] und können bequem gelesen und gespeichert werden.

Artikel 18: Den Verantwortlichen für die Verarbeitung personenbezogener Daten ist es gestattet, Personen nicht über die in Absatz 1 des vorstehenden Artikels genannten Punkte zu informieren, wenn Gesetze oder Verwaltungsvorschriften vorsehen, dass die Vertraulichkeit gewahrt bleibt oder eine Benachrichtigung nicht erforderlich ist.

In Notfällen, in denen es nicht möglich ist, natürliche Personen rechtzeitig zu benachrichtigen, um ihr Leben, ihre Gesundheit und die Sicherheit ihres Eigentums zu schützen, benachrichtigen die Verantwortlichen für die Verarbeitung personenbezogener Daten die Personen nach Abschluss der Notfälle.

Artikel 19: Sofern Gesetze oder Verwaltungsvorschriften nichts anderes vorsehen, ist die Aufbewahrungsfrist für personenbezogene Daten so kurz wie möglich zu halten, um den Zweck der Verarbeitung personenbezogener Daten zu erfüllen.

Artikel 20: Wenn zwei oder mehr Verantwortliche für die Verarbeitung personenbezogener Daten gemeinsam über den Zweck und die Art der Verarbeitung entscheiden, müssen sie sich über die Rechte und Pflichten jedes Einzelnen einigen. Diese Vereinbarung hat jedoch keinen Einfluss auf die Rechte einer Person, von einem der Verantwortlichen für die Verarbeitung personenbezogener Daten die Erfüllung der Bestimmungen dieses Gesetzes zu verlangen.

Artikel 21: Beauftragen die Verantwortlichen für die Verarbeitung personenbezogener Daten die Verarbeitung personenbezogener Daten, so schließen sie mit der beauftragten Person eine Vereinbarung über den Zweck der beauftragten Verarbeitung, die Frist, die Verarbeitungsmethode, die Kategorien personenbezogener Daten, die Schutzmaßnahmen sowie die Rechte und Pflichten beider Seiten usw. und führen eine Überwachung der Verarbeitung personenbezogener Daten durch die beauftragte Person durch.

Die beauftragten Personen müssen personenbezogene Daten gemäß der Vereinbarung verarbeiten; sie dürfen personenbezogene Daten nicht zu anderen Zwecken oder in anderen Verfahren verarbeiten, als in der Vereinbarung vorgesehen ist. Wenn der Vertrauensvertrag nicht in Kraft tritt, ungültig ist, gekündigt oder beendet wurde, muss die betraute Person die personenbezogenen Daten an den Verantwortlichen für die Verarbeitung personenbezogener Daten zurückgeben oder sie löschen und darf sie nicht zurückbehalten.

Ohne die Zustimmung des Verantwortlichen für die Verarbeitung personenbezogener Daten darf die beauftragte Person keine weiteren Personen mit der Verarbeitung personenbezogener Daten betrauen.

Artikel 22: Die Verantwortlichen für die Verarbeitung personenbezogener Daten müssen, wenn die Weitergabe personenbezogener Daten aufgrund von Fusionen, Trennungen, Auflösungen, Konkurserklärungen und anderen derartigen Gründen erforderlich ist, die Personen über den Namen oder den persönlichen Namen der empfangenden Partei und die Kontaktmethode informieren. Die empfangende Partei muss weiterhin die Pflichten des Bearbeiters der personenbezogenen Daten erfüllen. Ändert die empfangende Seite den ursprünglichen Verarbeitungszweck oder die Verarbeitungsmethode, muss sie die Person erneut gemäß den Bestimmungen dieses Gesetzes benachrichtigen.

Artikel 23: Wenn Verantwortliche für die Verarbeitung personenbezogener Daten anderen Verantwortlichen für die Verarbeitung personenbezogener Daten die von ihnen verarbeiteten personenbezogenen Daten zur Verfügung stellen, müssen sie die betroffenen Personen über den Namen oder den Personennamen des Empfängers, die Art der Kontaktaufnahme, den Zweck der Verarbeitung, die Art der Verarbeitung und die Kategorien der personenbezogenen Daten informieren und die gesonderte Zustimmung der betroffenen Person einholen. Die Empfänger müssen personenbezogene Daten innerhalb des oben genannten Rahmens von Verarbeitungszwecken, Verarbeitungsmethoden, Kategorien personenbezogener Daten usw. verarbeiten. Ändern die Empfänger den ursprünglichen Verarbeitungszweck oder die Verarbeitungsmethode, müssen sie erneut die Zustimmung der betroffenen Person einholen.

Artikel 24: Wenn Personen, die personenbezogene Daten verarbeiten, personenbezogene Daten zur automatisierten Entscheidungsfindung verwenden, müssen die Transparenz der Entscheidungsfindung und die Fairness und Gerechtigkeit des Verarbeitungsergebnisses gewährleistet sein, und sie dürfen keine unangemessene Ungleichbehandlung von Personen bei den Handelsbedingungen, wie z. B. dem Handelspreis, vornehmen.

Diejenigen, die mit Hilfe automatisierter Entscheidungsfindungsmethoden Push-Informationen liefern oder kommerzielle Verkäufe an Einzelpersonen tätigen, müssen gleichzeitig die Möglichkeit bieten, die Merkmale einer Person nicht zu berücksichtigen, oder der Person eine bequeme Methode zur Verweigerung anbieten.

Wenn der Einsatz automatisierter Entscheidungsfindung zu Entscheidungen führt, die einen großen Einfluss auf die Rechte und Interessen des Einzelnen haben, hat er das Recht, von den Verantwortlichen für die Verarbeitung personenbezogener Daten eine Erklärung zu verlangen, und er hat das Recht, sich zu weigern, dass die Verantwortlichen für die Verarbeitung personenbezogener Daten Entscheidungen ausschließlich durch automatisierte Entscheidungsfindungsmethoden treffen.

Artikel 25: Die Verantwortlichen für die Verarbeitung personenbezogener Daten dürfen die von ihnen verarbeiteten personenbezogenen Daten nicht weitergeben, es sei denn, sie erhalten eine gesonderte Einwilligung.

Artikel 26: Die Installation von Bildsammel- oder Personenerkennungsgeräten an öffentlichen Orten hat so zu erfolgen, wie es zum Schutz der öffentlichen Sicherheit und zur Einhaltung der einschlägigen staatlichen Vorschriften erforderlich ist, und es sind deutliche Hinweisschilder anzubringen. Gesammelte personenbezogene Bilder und Informationen über persönliche Identitätsmerkmale dürfen nur zum Schutz der öffentlichen Sicherheit verwendet werden; sie dürfen nicht für andere Zwecke verwendet werden, es sei denn, es liegt eine gesonderte Zustimmung der Betroffenen vor.

Artikel 27: Die mit der Verarbeitung personenbezogener Daten Beauftragten dürfen in einem angemessenen Rahmen personenbezogene Daten verarbeiten, die bereits von der Person selbst offengelegt wurden oder auf andere Weise rechtmäßig offengelegt wurden, es sei denn, die Person lehnt dies eindeutig ab. Personenbezogene Datenverarbeiter, die bereits offengelegte personenbezogene Daten verarbeiten, bei denen ein erheblicher Einfluss auf die Rechte und Interessen des Einzelnen besteht, müssen die persönliche Zustimmung gemäß den Bestimmungen dieses Gesetzes einholen.

Abschnitt II: Regeln für den Umgang mit sensiblen personenbezogenen Daten

Artikel 28: Sensible personenbezogene Daten sind personenbezogene Daten, die, wenn sie an die Öffentlichkeit gelangen oder unrechtmäßig verwendet werden, leicht die Würde natürlicher Personen verletzen und die persönliche oder materielle Sicherheit ernsthaft beeinträchtigen können, einschließlich Informationen über biometrische Merkmale, religiöse Überzeugungen, einen gekennzeichneten Status, den Gesundheitszustand, Finanzkonten, die Verfolgung des individuellen Standorts usw. sowie personenbezogene Daten von Minderjährigen unter 14 Jahren.

Nur in Fällen, in denen ein spezifischer Zweck und ein Bedarf besteht, und unter strengen Schutzmaßnahmen dürfen die für die Verarbeitung von personenbezogenen Daten Verantwortlichen mit sensiblen personenbezogenen Daten umgehen.

Artikel 29: Für die Verarbeitung sensibler personenbezogener Daten ist die gesonderte Zustimmung des Betroffenen einzuholen. Wenn Gesetze oder Verwaltungsvorschriften vorsehen, dass für die Verarbeitung sensibler personenbezogener Daten eine schriftliche Zustimmung eingeholt werden muss, sind diese Bestimmungen zu befolgen.

Artikel 30: Personen, die mit sensiblen persönlichen Daten umgehen, müssen zusätzlich zu den in Artikel 17, Absatz 1 dieses Gesetzes genannten Punkten auch die Personen über die Notwendigkeit und den Einfluss auf die Rechte und Interessen der Personen beim Umgang mit den sensiblen persönlichen Daten informieren, es sei denn, dieses Gesetz sieht vor, dass die Personen nicht informiert werden dürfen.

Artikel 31: Verarbeitet ein Verantwortlicher personenbezogene Daten von Minderjährigen unter 14 Jahren, so muss er die Zustimmung der Eltern oder eines anderen Vormunds des Minderjährigen einholen.

Verarbeiten Verantwortliche personenbezogene Daten von Minderjährigen unter 14 Jahren, so müssen sie spezielle Regeln für den Umgang mit personenbezogenen Daten aufstellen.

Artikel 32: Soweit Gesetze oder Verwaltungsvorschriften vorsehen, dass für den Umgang mit sensiblen personenbezogenen Daten entsprechende behördliche Genehmigungen eingeholt werden müssen oder andere Beschränkungen gelten, sind diese Bestimmungen zu befolgen.

Abschnitt III: Besondere Bestimmungen für den Umgang staatlicher Organe mit personenbezogenen Daten

Artikel 33: Dieses Gesetz gilt für den Umgang staatlicher Organe mit personenbezogenen Daten; soweit dieser Abschnitt besondere Bestimmungen enthält, gelten die Bestimmungen dieses Abschnitts.

Artikel 34: Staatliche Organe, die zur Erfüllung ihrer gesetzlichen Pflichten und Verantwortlichkeiten mit personenbezogenen Daten umgehen, haben dies gemäß den in Gesetzen oder Verwaltungsvorschriften vorgesehenen Befugnissen und Verfahren zu tun; sie dürfen nicht über den Umfang oder das Ausmaß hinausgehen, das zur Erfüllung ihrer gesetzlichen Pflichten und Verantwortlichkeiten erforderlich ist.

Artikel 35: Staatliche Organe, die personenbezogene Daten zur Erfüllung ihrer gesetzlichen Pflichten und Verantwortlichkeiten verarbeiten, sind zur Benachrichtigung verpflichtet, es sei denn, es liegen die in Artikel 18 Absatz I dieses Gesetzes genannten Umstände vor oder die Benachrichtigung behindert die staatlichen Organe bei der Erfüllung ihrer gesetzlichen Pflichten und Verantwortlichkeiten.

Artikel 36: Personenbezogene Daten, die von staatlichen Organen verarbeitet werden, sind auf dem Festlandgebiet der Volksrepublik China zu speichern. Wenn es unbedingt notwendig ist, sie ins Ausland zu übermitteln, ist eine Sicherheitsbewertung vorzunehmen. Die zuständigen Behörden können um Unterstützung und Hilfe bei der Sicherheitsüberprüfung gebeten werden.

Artikel 37: Die Bestimmungen dieses Gesetzes über den Umgang mit personenbezogenen Daten durch staatliche Organe gelten für den Umgang mit personenbezogenen Daten zur Erfüllung gesetzlicher Pflichten durch Organisationen, die durch Gesetze und Verordnungen ermächtigt sind, Aufgaben im Bereich öffentlicher Angelegenheiten wahrzunehmen.

Kapitel III: Vorschriften über die grenzüberschreitende Übermittlung personenbezogener Daten

Artikel 38: Wenn Personen, die personenbezogene Daten verarbeiten, aus geschäftlichen oder anderen Gründen tatsächlich personenbezogene Daten außerhalb der Grenzen der Volksrepublik China bereitstellen müssen, müssen sie eine der folgenden Bedingungen erfüllen:

1. Bestehen einer von der staatlichen Abteilung für Cybersicherheit und Informatisierung organisierten Sicherheitsprüfung gemäß Artikel 40 dieses Gesetzes;
2. Sie müssen sich einer Zertifizierung zum Schutz personenbezogener Daten unterziehen, die von einer spezialisierten Stelle gemäß den Bestimmungen der staatlichen Abteilung für Cybersicherheit und Informatisierung durchgeführt wird;
3. Abschluss eines Vertrags mit der ausländischen empfangenden Seite in Übereinstimmung mit einem Standardvertrag, der von der staatlichen Abteilung für Cyberspace und Informatisierung formuliert wurde, wobei die Rechte und Pflichten beider Seiten vereinbart werden;
4. Andere Bedingungen, die in Gesetzen oder Verwaltungsvorschriften oder von der staatlichen Abteilung für Cybersicherheit und Informatisierung vorgesehen sind.

Wenn Verträge oder internationale Abkommen, die die Volksrepublik China abgeschlossen hat oder denen sie beigetreten ist, einschlägige Bestimmungen enthalten, wie z. B. Bedingungen für die Bereitstellung personenbezogener Daten außerhalb der Grenzen der Volksrepublik China, können diese Bestimmungen umgesetzt werden.

Die für die Verarbeitung personenbezogener Daten Verantwortlichen haben die erforderlichen Maßnahmen zu ergreifen, um sicherzustellen, dass die Verarbeitung personenbezogener Daten durch ausländische Empfänger den in diesem Gesetz vorgesehenen Standard des Schutzes personenbezogener Daten erreicht.

Artikel 39: Wenn die für die Verarbeitung personenbezogener Daten Verantwortlichen personenbezogene Daten außerhalb der Grenzen der Volksrepublik China weitergeben, müssen sie die Person über den Namen oder den Personennamen des ausländischen Empfängers, die Kontaktmethode, den Zweck der Verarbeitung, die Verarbeitungsmethoden und die Kategorien der personenbezogenen Daten sowie über die Möglichkeiten und Verfahren informieren, mit denen die Person die in diesem Gesetz vorgesehenen Rechte gegenüber dem ausländischen Empfänger ausüben kann, und andere derartige Angelegenheiten mitteilen und die gesonderte Zustimmung der Person einholen.

Artikel 40: Die Betreiber kritischer Informationsinfrastrukturen und die für die Verarbeitung personenbezogener Daten Verantwortlichen, die die von der staatlichen Abteilung für Cybersicherheit und Informatisierung bereitgestellten Mengen erreichen, müssen die innerhalb der Grenzen der Volksrepublik China erhobenen und erzeugten personenbezogenen Daten im Inland speichern. Wenn sie diese ins Ausland weitergeben müssen, müssen sie eine vom Staatlichen Amt für Computer- und Netzsicherheit organisierte Sicherheitsprüfung bestehen; wo Gesetze oder Verwaltungsvorschriften und Bestimmungen des Staatlichen Amtes für Computer- und

Netzicherheit erlauben, dass keine Sicherheitsprüfung durchgeführt wird, sind diese Bestimmungen zu befolgen.

Artikel 41: Die zuständigen Behörden der Volksrepublik China haben gemäß den einschlägigen Gesetzen und Verträgen oder internationalen Abkommen, die die Volksrepublik China abgeschlossen hat oder denen sie beigetreten ist, oder gemäß dem Grundsatz der Gleichheit und des gegenseitigen Nutzens die Ersuchen ausländischer Justiz- oder Strafverfolgungsbehörden in Bezug auf die Bereitstellung von im Inland gespeicherten personenbezogenen Daten zu bearbeiten. Ohne die Genehmigung der zuständigen Behörden der Volksrepublik China dürfen die für die Verarbeitung personenbezogener Daten zuständigen Stellen keine im Festlandgebiet der Volksrepublik China gespeicherten personenbezogenen Daten an ausländische Justiz- oder Strafverfolgungsbehörden weitergeben.

Artikel 42: Wenn ausländische Organisationen oder Einzelpersonen bei der Verarbeitung personenbezogener Daten die Rechte und Interessen der Bürger der Volksrepublik China verletzen oder der nationalen Sicherheit oder dem öffentlichen Interesse der Volksrepublik China schaden, kann die staatliche Abteilung für Cybersicherheit und Informatisierung sie auf eine Liste setzen, die die Bereitstellung personenbezogener Daten einschränkt oder verbietet, eine Warnung aussprechen und Maßnahmen wie die Einschränkung oder das Verbot der Bereitstellung personenbezogener Daten an sie ergreifen usw.

Artikel 43: Wenn ein Land oder eine Region diskriminierende Verbote, Beschränkungen oder andere ähnliche Maßnahmen gegen die Volksrepublik China im Bereich des Schutzes personenbezogener Daten ergreift, kann die Volksrepublik China auf der Grundlage der tatsächlichen Umstände Gegenmaßnahmen gegen dieses Land oder diese Region ergreifen.

Kapitel IV: Rechte des Einzelnen bei der Verarbeitung personenbezogener Daten

Artikel 44: Der Einzelne hat das Recht, seine persönlichen Daten zu kennen und darüber zu entscheiden, und er hat das Recht, die Verarbeitung seiner persönlichen Daten durch andere einzuschränken oder zu verweigern, sofern nicht Gesetze oder Verwaltungsvorschriften etwas anderes vorschreiben.

Artikel 45: Der Einzelne hat das Recht, seine persönlichen Daten bei den Bearbeitern einzusehen und zu kopieren, außer unter den in Artikel 18, Absatz 1, oder Artikel 35 dieses Gesetzes vorgesehenen Umständen.

Beantragt eine Person Einsicht in ihre persönlichen Daten oder eine Kopie davon, so ist der Bearbeiter von personenbezogenen Daten verpflichtet, diese rechtzeitig zur Verfügung zu stellen.

Beantragt eine Person die Übermittlung ihrer personenbezogenen Daten an einen von ihr benannten Bearbeiter, der die Bedingungen des staatlichen Amtes für Cybersicherheit und Informatisierung erfüllt, so muss der Bearbeiter von personenbezogenen Daten einen Kanal für die Übermittlung bereitstellen.

Artikel 46: Stellt eine Person fest, dass ihre personenbezogenen Daten unrichtig oder unvollständig sind, hat sie das Recht, von dem Verantwortlichen für die Verarbeitung personenbezogener Daten die Berichtigung oder Vervollständigung ihrer personenbezogenen Daten zu verlangen. Beantragt eine Person die Berichtigung oder Vervollständigung ihrer personenbezogenen Daten, so überprüft der Verantwortliche für die Verarbeitung personenbezogener Daten die personenbezogenen Daten und berichtigt oder vervollständigt sie zügig.

Beantragt eine Person die Berichtigung oder Vervollständigung ihrer personenbezogenen Daten, so überprüft der Verantwortliche für die Verarbeitung personenbezogener Daten die personenbezogenen Daten und berichtigt oder vervollständigt sie zeitnah.

Artikel 47: Die Verantwortlichen für die Verarbeitung personenbezogener Daten müssen personenbezogene Daten proaktiv löschen, wenn einer der folgenden Umstände eintritt; wenn der Verantwortliche für die Verarbeitung personenbezogener Daten sie nicht gelöscht hat, haben die Personen das Recht, die Löschung zu verlangen:

1. Der Zweck der Verarbeitung wurde erreicht, ist unmöglich zu erreichen, oder [die personenbezogenen Daten] sind nicht mehr notwendig, um den Zweck der Verarbeitung zu erreichen;
2. Die Verantwortlichen für die Verarbeitung personenbezogener Daten stellen die Bereitstellung von Produkten oder Dienstleistungen ein, oder die Aufbewahrungsfrist ist abgelaufen;
3. Die Person widerruft ihre Zustimmung;
4. Der Verarbeiter hat personenbezogene Daten unter Verletzung von Gesetzen, Verwaltungsvorschriften oder Vereinbarungen verarbeitet;
5. andere in Gesetzen oder Verwaltungsvorschriften vorgesehene Umstände.

Ist die in den Gesetzen oder Verwaltungsvorschriften vorgesehene Aufbewahrungsfrist noch nicht abgelaufen oder ist die Löschung personenbezogener Daten technisch schwer durchführbar, haben die Verantwortlichen für die Verarbeitung personenbezogener Daten die Verarbeitung personenbezogener Daten einzustellen, mit Ausnahme der Speicherung und der Ergreifung der erforderlichen Sicherheitsmaßnahmen.

Artikel 48: Der Einzelne hat das Recht, von den Verantwortlichen für die Verarbeitung personenbezogener Daten eine Erläuterung der Regeln für die Verarbeitung personenbezogener Daten zu verlangen.

Artikel 49: Wenn eine natürliche Person verstorben ist, können ihre nächsten Angehörigen zur Wahrung ihrer eigenen rechtmäßigen und legitimen Interessen die in diesem Kapitel vorgesehenen Rechte auf Einsichtnahme, Kopie, Berichtigung, Löschung usw. der personenbezogenen Daten der verstorbenen Person ausüben, es sei denn, die verstorbene Person hat vor ihrem Tod etwas anderes vereinbart.

Artikel 50: Die für die Verarbeitung personenbezogener Daten Verantwortlichen richten geeignete Mechanismen ein, um Anträge von Personen auf Ausübung ihrer Rechte anzunehmen und zu bearbeiten. Lehnen sie Anträge von Personen auf Ausübung ihrer Rechte ab, so haben sie dies zu begründen.

Lehnt der Verantwortliche für die Verarbeitung personenbezogener Daten den Antrag einer Person auf Ausübung ihrer Rechte ab, kann diese Person gemäß dem Gesetz Klage beim Volksgericht erheben.

Kapitel V: Pflichten der für die Verarbeitung personenbezogener Daten Verantwortlichen

Artikel 51: Die Verantwortlichen für die Verarbeitung personenbezogener Daten müssen auf der Grundlage des Zwecks der Verarbeitung personenbezogener Daten, der Verarbeitungsmethoden, der Kategorien personenbezogener Daten sowie des Einflusses auf die Rechte und Interessen von Einzelpersonen, möglicherweise bestehender Sicherheitsrisiken usw. die folgenden Maßnahmen ergreifen, um sicherzustellen, dass die Verarbeitung personenbezogener Daten den Bestimmungen der Gesetze und Verwaltungsvorschriften entspricht, und um unbefugten Zugriff sowie die Weitergabe, Verfälschung oder den Verlust personenbezogener Daten zu verhindern:

1. Formulierung interner Managementstrukturen und Betriebsregeln;
2. Implementierung eines kategorisierten Managements persönlicher Informationen;
3. Ergreifen entsprechender technischer Sicherheitsmaßnahmen wie Verschlüsselung, De-Identifizierung usw.;
4. Angemessene Festlegung von Betriebsgrenzen für den Umgang mit personenbezogenen Daten und regelmäßige Durchführung von Sicherheitsschulungen und -trainings für Mitarbeiter;
5. Formulierung und Organisation der Umsetzung von Plänen zur Reaktion auf Sicherheitsvorfälle mit personenbezogenen Daten;
6. Andere Maßnahmen, die in Gesetzen oder Verwaltungsvorschriften vorgesehen sind.

Artikel 52: Personenbezogene Datenverarbeiter, die personenbezogene Daten verarbeiten und dabei die von der staatlichen Abteilung für Cybersicherheit und Informatisierung zur Verfügung gestellten Mengen erreichen, müssen Datenschutzbeauftragte ernennen, die für die Überwachung der Tätigkeiten zur Verarbeitung personenbezogener Daten sowie für die angenommenen Schutzmaßnahmen usw. verantwortlich sind.

Die Verantwortlichen für den Umgang mit personenbezogenen Daten müssen die Methoden zur Kontaktaufnahme mit den Beauftragten für den Schutz personenbezogener Daten bekannt geben und die Namen der Beauftragten und die Kontaktmethoden an die Abteilungen melden, die für den Schutz personenbezogener Daten zuständig sind und Verantwortung tragen.

Artikel 53: Personen, die außerhalb der Grenzen der Volksrepublik China mit personenbezogenen Daten umgehen, müssen gemäß Artikel 3, Absatz 2 dieses Gesetzes eine spezielle Stelle einrichten oder einen Vertreter innerhalb der Grenzen der Volksrepublik China ernennen, der für die Angelegenheiten im Zusammenhang mit den von ihnen behandelten personenbezogenen Daten verantwortlich ist, und müssen den Namen der entsprechenden Stelle oder den Namen des Vertreters und die Kontaktmethode usw. den Abteilungen mitteilen, die für den Schutz personenbezogener Daten zuständig und verantwortlich sind.

Artikel 54: Die Verantwortlichen für den Umgang mit personenbezogenen Daten führen regelmäßig Audits über den Umgang mit personenbezogenen Daten und die Einhaltung der Gesetze und Verwaltungsvorschriften durch.

Artikel 55: Wenn einer der folgenden Umstände vorliegt, müssen die Verantwortlichen für den Umgang mit personenbezogenen Daten im Voraus eine Folgenabschätzung für den Schutz personenbezogener Daten durchführen und die Situation des Umgangs mit diesen Daten dokumentieren:

1. Umgang mit sensiblen personenbezogenen Daten;
2. Verwendung personenbezogener Daten zur automatisierten Entscheidungsfindung;
3. Beauftragung mit der Verarbeitung personenbezogener Daten, Weitergabe personenbezogener Daten an andere Verarbeiter personenbezogener Daten oder Offenlegung personenbezogener Daten
4. Bereitstellung von personenbezogenen Daten im Ausland;
5. Andere Tätigkeiten im Umgang mit personenbezogenen Daten, die einen großen Einfluss auf Personen haben.

Artikel 56: Der Inhalt der Folgenabschätzung zum Schutz personenbezogener Daten muss Folgendes umfassen:

1. Ob der Zweck der Verarbeitung personenbezogener Daten, die Art der Verarbeitung usw. rechtmäßig, legitim und notwendig sind oder nicht;
2. Der Einfluss auf die Rechte und Interessen des Einzelnen und die Sicherheitsrisiken;
3. ob die getroffenen Schutzmaßnahmen rechtmäßig, wirksam und dem Risiko angemessen sind.

Die Berichte über die Folgenabschätzung zum Schutz personenbezogener Daten und die Aufzeichnungen über den Bearbeitungsstatus sind mindestens drei Jahre lang aufzubewahren.

Artikel 57: Wenn ein Leck, eine Verfälschung oder ein Verlust personenbezogener Daten auftritt oder aufgetreten sein könnte, ergreifen die für die Verarbeitung personenbezogener Daten Verantwortlichen unverzüglich Abhilfemaßnahmen und benachrichtigen die Abteilungen, die für den Schutz personenbezogener Daten verantwortlich sind, sowie die betroffenen Personen. Die Benachrichtigung muss die folgenden Punkte enthalten:

1. Die Informationskategorien, die Ursachen und die möglichen Schäden, die durch das Leck, die Verfälschung oder den Verlust entstanden sind oder entstanden sein könnten;
2. die vom Verantwortlichen für die Verarbeitung personenbezogener Daten getroffenen Abhilfemaßnahmen und die Maßnahmen, die Einzelpersonen zur Schadensbegrenzung ergreifen können;
3. Kontaktmöglichkeiten mit dem Verantwortlichen für die Verarbeitung personenbezogener Daten.

Wenn der Verantwortliche für die Verarbeitung personenbezogener Daten Maßnahmen ergreift, die in der Lage sind, den durch das Austreten, die Verfälschung oder den Verlust von Informationen entstandenen Schaden wirksam zu vermeiden, ist es dem Verantwortlichen für die Verarbeitung personenbezogener Daten gestattet, die Personen nicht zu benachrichtigen; wenn jedoch die Abteilungen, die die Pflichten und Verantwortlichkeiten zum Schutz personenbezogener Daten wahrnehmen, der Meinung sind, dass ein Schaden entstanden sein könnte, können sie vom Verantwortlichen für die Verarbeitung personenbezogener Daten verlangen, die Personen zu benachrichtigen.

Artikel 58: Personenbezogene Datenverarbeiter, die wichtige Dienste auf Internetplattformen anbieten, die eine große Anzahl von Nutzern haben und deren Geschäftsmodelle komplex sind, müssen die folgenden Verpflichtungen erfüllen:

1. Einrichtung und Vervollständigung von Systemen und Strukturen zur Einhaltung des Schutzes personenbezogener Daten gemäß den staatlichen Vorschriften und Einrichtung eines unabhängigen Gremiums, das sich hauptsächlich aus externen Mitgliedern zusammensetzt, um die Umstände des Schutzes personenbezogener Daten zu überwachen;
2. sich an die Grundsätze der Offenheit, Fairness und Gerechtigkeit zu halten, Plattformregeln zu formulieren und die Standards für den Umgang von Produkt- oder Diensteanbietern innerhalb der Plattform mit personenbezogenen Daten und ihre Pflichten zum Schutz personenbezogener Daten zu klären;
3. Beenden Sie die Bereitstellung von Diensten für Produkt- oder Dienstleistungsanbieter auf der Plattform, die ernsthaft gegen Gesetze oder Verwaltungsvorschriften im Umgang mit personenbezogenen Daten verstoßen;
4. Regelmäßige Veröffentlichung von Berichten über die soziale Verantwortung im Bereich des Schutzes personenbezogener Daten und Akzeptanz der Überwachung durch die Gesellschaft.

Artikel 59: Beauftragte Personen, die den Umgang mit personenbezogenen Daten übernehmen, müssen gemäß den Bestimmungen dieses Gesetzes und den einschlägigen Gesetzen und Verwaltungsvorschriften die notwendigen Maßnahmen ergreifen, um die Sicherheit der von ihnen bearbeiteten personenbezogenen Daten zu gewährleisten, und die Bearbeiter personenbezogener Daten bei der Erfüllung der in diesem Gesetz vorgesehenen Pflichten unterstützen.

Kapitel VI: Abteilungen, die Aufgaben und Verantwortlichkeiten im Bereich des Schutzes personenbezogener Daten wahrnehmen

Artikel 60: Die staatliche Abteilung für Cybersicherheit und Informatisierung ist für die umfassende Planung und Koordinierung der Arbeit zum Schutz personenbezogener Daten und der damit verbundenen Aufsichts- und Verwaltungsarbeit verantwortlich. Die zuständigen Abteilungen des Staatsrats sind für den Schutz, die Überwachung und die Verwaltung personenbezogener Daten in ihrem jeweiligen Aufgaben- und Verantwortungsbereich gemäß den Bestimmungen dieses Gesetzes und den einschlägigen Gesetzen und Verwaltungsvorschriften verantwortlich.

Die Aufgaben und Zuständigkeiten der für den Schutz, die Überwachung und die Verwaltung personenbezogener Daten zuständigen Abteilungen der Bezirksregierungen und höherer Volksregierungen werden gemäß den einschlägigen staatlichen Bestimmungen festgelegt.

Die in den beiden vorangegangenen Absätzen genannten Dienststellen werden alle als Dienststellen bezeichnet, die Aufgaben und Verantwortlichkeiten im Bereich des Schutzes personenbezogener Daten wahrnehmen.

Artikel 61: Die Abteilungen, die Aufgaben und Verantwortlichkeiten im Bereich des Schutzes persönlicher Daten erfüllen, haben folgende Aufgaben und Verantwortlichkeiten im Bereich des Schutzes persönlicher Daten:

1. Durchführung von Propaganda und Aufklärung über den Schutz personenbezogener Daten sowie Anleitung und Überwachung der Arbeit von Personen, die mit dem Schutz personenbezogener Daten zu tun haben;
2. Entgegennahme und Bearbeitung von Beschwerden und Berichten über den Schutz personenbezogener Daten;
3. Organisation der Bewertung der Situation des Schutzes personenbezogener Daten, z. B. der angewandten Verfahren, und Veröffentlichung der Bewertungsergebnisse.
4. Untersuchung von und Umgang mit ungesetzlichen Aktivitäten im Umgang mit personenbezogenen Daten;
5. Andere Pflichten und Verantwortlichkeiten, die in Gesetzen oder Verwaltungsvorschriften vorgesehen sind.

Artikel 62: Die staatliche Abteilung für Cybersicherheit und Informatisierung koordiniert insgesamt die folgenden Arbeiten zum Schutz personenbezogener Daten durch die zuständigen Abteilungen:

1. Formulierung konkreter Regeln und Standards für den Schutz personenbezogener Daten;
2. Formulierung spezieller Regeln und Standards für den Schutz persönlicher Daten für kleine Unternehmen, die persönliche Daten verarbeiten, sowie für neue Technologien und neue Anwendungen für den Umgang mit sensiblen persönlichen Daten, Gesichtserkennung, künstliche Intelligenz usw.;
3. Unterstützung der Forschung, Entwicklung und breiten Einführung sicherer und bequemer elektronischer Identitätsauthentifizierungstechnologien und Förderung des Aufbaus von öffentlichen Online-Identitätsauthentifizierungsdiensten;
4. Förderung des Aufbaus von Dienstleistungssystemen zum Schutz personenbezogener Daten und Unterstützung relevanter Organisationen bei der Einführung von Bewertungs- und Zertifizierungsdiensten zum Schutz personenbezogener Daten;
5. Perfektionierung der Beschwerde- und Meldemechanismen zum Schutz personenbezogener Daten.

Artikel 63: Wenn Abteilungen, die Pflichten und Verantwortlichkeiten im Bereich des Schutzes persönlicher Daten erfüllen, können sie die folgenden Maßnahmen ergreifen:

1. Befragung der betroffenen Parteien und Untersuchung der Umstände im Zusammenhang mit der Verarbeitung personenbezogener Daten;

2. Einsichtnahme in und Vervielfältigung von Verträgen, Aufzeichnungen und Belegen einer betroffenen Partei sowie anderer relevanter Materialien im Zusammenhang mit der Verarbeitung personenbezogener Daten;
3. Durchführung von Vor-Ort-Inspektionen und Ermittlungen bei Verdacht auf unrechtmäßigen Umgang mit personenbezogenen Daten;
4. Inspektion von Ausrüstungen und Gegenständen, die für den Umgang mit personenbezogenen Daten relevant sind; wenn es Beweise dafür gibt, dass die Ausrüstungen oder Gegenstände für illegale Tätigkeiten im Umgang mit personenbezogenen Daten verwendet werden, können sie diese versiegeln oder beschlagnahmen, nachdem sie dem Hauptverantwortlichen ihrer Abteilung schriftlich Bericht erstattet und die Genehmigung erhalten haben.

Wenn Abteilungen, die Aufgaben und Verantwortlichkeiten im Bereich des Schutzes personenbezogener Daten wahrnehmen, ihre Aufgaben und Verantwortlichkeiten gemäß dem Gesetz erfüllen, müssen die betroffenen Parteien Unterstützung und Zusammenarbeit leisten und dürfen sie nicht behindern oder behindern.

Artikel 64: Stellen die für den Schutz personenbezogener Daten zuständigen Stellen fest, dass bei der Verarbeitung personenbezogener Daten relativ große Risiken bestehen oder dass es zu Sicherheitsvorfällen bei der Verarbeitung personenbezogener Daten kommt, können sie gemäß den gesetzlichen Befugnissen und Verfahren ein Gespräch mit dem gesetzlichen Vertreter oder dem Hauptverantwortlichen des Verantwortlichen für die Verarbeitung personenbezogener Daten führen oder von den Verantwortlichen für die Verarbeitung personenbezogener Daten verlangen, dass sie spezialisierte Einrichtungen mit der Durchführung von Konformitätsprüfungen ihrer Tätigkeiten zur Verarbeitung personenbezogener Daten beauftragen. Die Verantwortlichen für den Umgang mit personenbezogenen Daten ergreifen die erforderlichen Maßnahmen, um die Angelegenheit zu korrigieren und die Schwachstelle zu beseitigen.

Stellen die mit dem Schutz personenbezogener Daten betrauten Dienststellen im Rahmen ihrer Aufgaben einen unrechtmäßigen Umgang mit personenbezogenen Daten fest, bei dem der Verdacht besteht, dass er eine Straftat darstellt, so leiten sie die Angelegenheit unverzüglich an die für die öffentliche Sicherheit zuständigen Behörden weiter, damit diese die Angelegenheit gemäß den gesetzlichen Bestimmungen bearbeiten.

Artikel 65: Jede Organisation oder Einzelperson hat das Recht, bei den Stellen, die für den Schutz personenbezogener Daten zuständig sind, eine Beschwerde oder einen Bericht über unrechtmäßige Tätigkeiten im Umgang mit personenbezogenen Daten einzureichen. Die Dienststellen, die Beschwerden oder Meldungen entgegennehmen, bearbeiten diese unverzüglich und gesetzeskonform und unterrichten die beschwerdeführende oder meldende Person über das Ergebnis der Bearbeitung.

Die Dienststellen, die Aufgaben und Zuständigkeiten im Bereich des Schutzes personenbezogener Daten wahrnehmen, veröffentlichen Kontaktmöglichkeiten für die Entgegennahme von Beschwerden und Meldungen.

Kapitel VII: Gesetzliche Haftung

Artikel 66: Wenn personenbezogene Daten unter Verletzung dieses Gesetzes verarbeitet werden oder personenbezogene Daten verarbeitet werden, ohne dass die Pflichten zum Schutz personenbezogener Daten gemäß den Bestimmungen dieses Gesetzes erfüllt werden, müssen die Abteilungen, die die Pflichten und Verantwortlichkeiten zum Schutz personenbezogener Daten erfüllen, die Korrektur anordnen, die unrechtmäßigen Einnahmen beschlagnahmen und die vorläufige Aussetzung oder Beendigung der Erbringung von Dienstleistungen der Anwendungsprogramme, die unrechtmäßig personenbezogene Daten verarbeiten, anordnen; wenn die Korrektur verweigert wird, muss zusätzlich eine Geldstrafe von höchstens 1 Million Yuan verhängt werden; die direkt verantwortliche Person und andere direkt verantwortliche Mitarbeiter müssen eine Geldstrafe zwischen 10.000 und 100.000 Yuan zahlen.

Wenn die Umstände der im vorstehenden Absatz genannten rechtswidrigen Handlungen schwerwiegend sind, müssen die für den Schutz personenbezogener Daten zuständigen Abteilungen auf Provinz- oder höherer Ebene Korrekturen anordnen, die rechtswidrigen Einnahmen beschlagnahmen und eine Geldstrafe von höchstens 50 Millionen Yuan oder 5 % der Jahreseinnahmen verhängen. Sie können auch die Aussetzung der entsprechenden Geschäftstätigkeiten oder die Einstellung des Geschäftsbetriebs zur Berichtigung anordnen und der jeweils zuständigen Abteilung die Aufhebung der entsprechenden Verwaltungslizenzen oder die Aufhebung der Geschäftslizenzen melden. Gegen die direkt verantwortliche Person und andere direkt verantwortliche Mitarbeiter werden Geldstrafen zwischen 100.000 und 1 Million Yuan verhängt, und es kann auch beschlossen werden, dass sie für eine bestimmte Zeit keine Positionen als Direktor, Vorgesetzter, hochrangiger Manager oder Datenschutzbeauftragter bekleiden dürfen.

Artikel 67: Rechtswidrige Handlungen, die in diesem Gesetz vorgesehen sind, werden gemäß den einschlägigen Gesetzen und Verwaltungsvorschriften in Kreditakten eingetragen und veröffentlicht.

Artikel 68: Wenn staatliche Organe die in diesem Gesetz vorgesehenen Pflichten zum Schutz personenbezogener Daten nicht erfüllen, ordnen die ihnen übergeordneten Organe oder die Abteilungen, die Aufgaben und Verantwortlichkeiten im Bereich des Schutzes personenbezogener Daten wahrnehmen, eine Korrektur an; die unmittelbar verantwortliche Person und andere unmittelbar verantwortliche Personen sind gemäß dem Gesetz zu bestrafen.

Wenn das Personal von Abteilungen, die Aufgaben zum Schutz personenbezogener Daten wahrnehmen, seine Pflichten vernachlässigt, seine Macht missbraucht oder Vetternwirtschaft betreibt, was jedoch noch keine Straftat darstellt, wird es nach dem Gesetz bestraft.

Artikel 69: Wenn der Umgang mit personenbezogenen Daten die Rechte und Interessen der Betroffenen verletzt und zu einem Schaden führt und die Verantwortlichen für den Umgang mit personenbezogenen Daten nicht nachweisen können, dass sie keine Schuld trifft, müssen sie für die Verletzung der Rechte und Interessen der Betroffenen Schadenersatz leisten und die Verantwortung dafür übernehmen.

In der obigen Klausel wird die Verantwortung für die Entschädigung für die Verletzung nach dem daraus resultierenden Verlust für den Einzelnen oder dem daraus resultierenden Nutzen für den Bearbeiter personenbezogener Daten bestimmt. Sind der Schaden für den Einzelnen und der Nutzen

für den Verantwortlichen für die Verarbeitung personenbezogener Daten schwer zu bestimmen, so ist die Entschädigung entsprechend den praktischen Bedingungen festzulegen.

Artikel 70: Wenn Personen, die personenbezogene Daten verarbeiten, gegen die Bestimmungen dieses Gesetzes verstoßen und dadurch die Rechte und Vorteile vieler Einzelpersonen verletzen, können die Volksstaatsanwaltschaft, die gesetzlich bestimmten Verbraucherorganisationen und die von der staatlichen Abteilung für Cybersicherheit und Informatisierung benannten Organisationen gemäß dem Gesetz Klage bei einem Volksgericht erheben.

Artikel 71: Stellt ein Verstoß gegen die Bestimmungen dieses Gesetzes einen Verstoß gegen die Verwaltung der öffentlichen Sicherheit dar, so wird die Verwaltung der öffentlichen Sicherheit gemäß dem Gesetz bestraft; handelt es sich um ein Verbrechen, so wird die strafrechtliche Verantwortung gemäß dem Gesetz untersucht.

Kapitel VIII: Ergänzende Bestimmungen

Artikel 72: Dieses Gesetz gilt nicht für natürliche Personen, die personenbezogene Daten für persönliche oder familiäre Angelegenheiten verarbeiten.

Soweit das Gesetz Bestimmungen über den Umgang mit personenbezogenen Daten durch die Volksregierungen auf allen Ebenen und ihre zuständigen Abteilungen und Organisationen, die statistische und archivarische Verwaltungstätigkeiten durchführen, enthält, gelten diese Bestimmungen.

Artikel 73: Die folgenden in diesem Gesetz verwendeten Begriffe werden wie folgt definiert:

1. "Verantwortlicher für die Verarbeitung personenbezogener Daten" bezieht sich auf Organisationen und Einzelpersonen, die bei der Verarbeitung personenbezogener Daten selbständig über die Zwecke der Verarbeitung entscheiden.
2. "Automatisierte Entscheidungsfindung" bezieht sich auf die Verwendung von Computerprogrammen zur automatischen Analyse oder Bewertung des persönlichen Verhaltens, der Gewohnheiten, Interessen oder Hobbys oder des Finanz-, Gesundheits-, Kredit- oder sonstigen Status und die darauf basierende Entscheidungsfindung.
3. "De-Identifizierung" bezieht sich auf den Prozess, bei dem personenbezogene Daten so bearbeitet werden, dass eine Identifizierung bestimmter natürlicher Personen ohne zusätzliche Informationen unmöglich ist.
4. "Anonymisierung" bezieht sich auf den Vorgang, bei dem personenbezogene Daten so verarbeitet werden, dass eine Unterscheidung zwischen bestimmten natürlichen Personen und eine Wiederherstellung unmöglich ist.

Artikel 74: Dieses Gesetz tritt am 1. November 2021 in Kraft.