



EUROPÄISCHE
KOMMISSION

Brüssel, den 26.1.2026
C(2026) 373 final

DURCHFÜHRUNGSBESCHLUSS DER KOMMISSION

vom 26.1.2026

**nach der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zur
Angemessenheit des Schutzes personenbezogener Daten durch Brasilien**

(Text von Bedeutung für den EWR)

DURCHFÜHRUNGSBESCHLUSS DER KOMMISSION

vom 26.1.2026

nach der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch Brasilien

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)¹, insbesondere auf Artikel 45 Absatz 3,

in Erwägung nachstehender Gründe:

1. EINLEITUNG

- (1) Die Verordnung (EU) 2016/679 enthält die Vorschriften für die Übermittlung personenbezogener Daten durch Verantwortliche oder Auftragsverarbeiter in der Union an Drittländer und internationale Organisationen, soweit die betreffenden Übermittlungen in ihren Anwendungsbereich fallen. Die Vorschriften über internationale Datenübermittlung sind in Kapitel V (Artikel 44 bis 50) der Verordnung festgelegt. Der Fluss personenbezogener Daten in Drittländer und aus Drittländern ist zwar für die Ausweitung des grenzüberschreitenden Handels und der internationalen Zusammenarbeit von wesentlicher Bedeutung, dennoch darf das unionsweit gewährleistete Schutzniveau für personenbezogene Daten bei Übermittlungen in Drittländer nicht untergraben werden².
- (2) Nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 kann die Kommission im Wege eines Durchführungsrechtsaktes beschließen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau bieten. Unter dieser Voraussetzung können personenbezogene Daten nach Artikel 45 Absatz 1 und Erwägungsgrund 103 der Verordnung (EU) 2016/679 ohne weitere Genehmigung an ein Drittland übermittelt werden.
- (3) Wie in Artikel 45 Absatz 2 der Verordnung (EU) 2016/679 festgelegt, muss die Annahme eines Angemessenheitsbeschlusses auf einer umfassenden Analyse der Rechtsordnung des Drittlands beruhen, und zwar sowohl in Bezug auf die für die Datenimporteure geltenden Vorschriften als auch auf die Einschränkungen und Garantien für den Zugang der Behörden zu personenbezogenen Daten. Im Rahmen ihrer Prüfung muss die Kommission feststellen, ob das betreffende Drittland ein

¹ ABL L 119 vom 4.5.2016, S. 1.

² Erwägungsgrund 101 der Verordnung (EU) 2016/679.

Schutzniveau garantiert, das dem innerhalb der Europäischen Union gewährleisteten Schutzniveau „der Sache nach gleichwertig“ ist³. Die Frage, ob ein Schutzniveau „der Sache nach gleichwertig“ ist, wird anhand des Maßstabs beurteilt, der in den Rechtsvorschriften der Europäischen Union, insbesondere in der Verordnung (EU) 2016/679, festgelegt und durch die Rechtsprechung des Gerichtshofs der Europäischen Union entwickelt wurde⁴. Eine weitere Orientierungshilfe bietet die „Referenzgrundlage für Angemessenheit“ des Europäischen Datenschutzausschusses (EDSA), mit der dieser Standard weiter präzisiert werden soll⁵.

- (4) Wie der Gerichtshof der Europäischen Union klargestellt hat, kann von einem Drittland nicht verlangt werden, ein Schutzniveau zu gewährleisten, das mit dem in der Rechtsordnung der Union garantierten Schutzniveau identisch ist⁶. Insbesondere können sich die Mittel, auf die das betreffende Drittland für den Schutz personenbezogener Daten zurückgreift, von denen unterscheiden, die in der Union herangezogen werden, sofern sie sich in der Praxis als wirksam erweisen, um ein angemessenes Schutzniveau zu gewährleisten⁷. Daher erfordert die Angemessenheitsfeststellung keine Eins-zu-eins-Übereinstimmung mit den Vorschriften der Union. Die Frage ist vielmehr, ob das ausländische System insgesamt aufgrund des Wesensgehalts der Rechte auf Privatsphäre und der Datenschutzgarantien (einschließlich ihrer wirksamen Anwendung, Überwachung und Durchsetzung) sowie aufgrund der Umstände, unter denen die personenbezogenen Daten übermittelt werden, das erforderliche Maß an Schutz bietet⁸.
 - (5) Die Kommission hat Recht und Praxis der Föderativen Republik Brasilien (im Folgenden „Brasilien“) analysiert. Ausgehend von den Feststellungen in den Erwägungsgründen 7 bis 223 gelangt die Kommission zu dem Schluss, dass Brasilien ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die im Rahmen der Verordnung (EU) 2016/679 aus der Union nach Brasilien übermittelt werden.
 - (6) Der Beschluss hat zur Folge, dass die Datenübermittlungen von Verantwortlichen und Auftragsverarbeitern in der Union an die Verantwortlichen und Auftragsverarbeiter in Brasilien ohne weitere Genehmigung vorgenommen werden können. Er wirkt sich nicht auf die unmittelbare Anwendung der Verordnung (EU) 2016/679 auf derartige Rechtsträger aus, wenn die in Artikel 3 der Verordnung festgelegten Bedingungen für den räumlichen Anwendungsbereich der Verordnung erfüllt sind.
2. VORSCHRIFTEN FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN
- 2.1. Der verfassungsrechtliche Rahmen Brasiliens
- (7) Brasilien ist eine Föderative Republik, die sich aus 26 Bundesstaaten und dem Bundesdistrikt zusammensetzt, wie in ihrer Bundesverfassung (im Folgenden „Verfassung“)⁹ festgelegt ist. Die brasilianischen Bundesstaaten verfügen auch über

³ Erwägungsgrund 104 der Verordnung (EU) 2016/679.

⁴ Rechtssache C-311/18, Facebook Ireland/Schrems (im Folgenden „Schrems II“), ECLI:EU:C:2020:559.

⁵ Europäischer Datenschutzausschuss, Referenzgrundlage für Angemessenheit, WP 254 Rev. 01. Abrufbar unter: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

⁶ Rechtssache C-362/14, Schrems (im Folgenden „Schrems I“), ECLI:EU:C:2015:650, Rn. 73.

⁷ Schrems I, Rn. 74.

⁸ Schrems I, Rn. 75.

⁹ Verfassung der Föderativen Republik Brasilien von 1988. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

eigene Verfassungen, die nicht im Widerspruch zur Bundesverfassung¹⁰ stehen dürfen. Brasilien verfügt über ein Präsidialsystem, in dem der Präsident und die Mitglieder der gesetzgebenden Kammern (d. h. die Abgeordnetenversammlung und der Bundessenat) direkt gewählt werden.

- (8) Die Privatsphäre und der Datenschutz sind in der Verfassung als Grundrechte geschützt. Insbesondere schützt Artikel 5 Ziffer X der Verfassung die Privatsphäre und das Privatleben natürlicher Personen, Artikel 5 Ziffer XII gewährleistet das Briefgeheimnis, einschließlich des Datenaustauschs, und Artikel 5 Ziffer LXXIX legt das Recht auf den Schutz personenbezogener Daten online und offline fest¹¹.
- (9) Alle in der Verfassung verankerten Rechte gelten gemäß Artikel 5 der Verfassung für brasilianische Staatsangehörige und Ausländer, die ihren Wohnsitz in Brasilien haben. Durch Bundesgesetze wird klargestellt, dass jede Person im Hoheitsgebiet Brasiliens – unabhängig davon, ob sie dort ihren Wohnsitz hat oder nicht – Anspruch auf den Schutz der Grundrechte hat¹². Der Umfang des Schutzes dieser Rechte wurde durch die verfassungsrechtliche Rechtsprechung auf im Ausland lebende Ausländer ausgeweitet, wie auch in der einschlägigen Rechtslehre hervorgehoben wird¹³. Folglich kann sich jeder Ausländer, unabhängig davon, ob er seinen Wohnsitz in Brasilien hat oder nicht, auf diesen verfassungsrechtlichen Schutz berufen¹⁴.
- (10) Brasilien ratifizierte 1992 die Amerikanische Menschenrechtskonvention, bekannt als „Pakt von San José“¹⁵ (im Folgenden „Konvention“). Unter anderem garantiert Artikel 11 der Konvention das Recht auf Privatsphäre und Artikel 8 schützt das Recht auf ein faires Verfahren. Im Jahr 1998 erkannte Brasilien die verbindliche Autorität des Interamerikanischen Gerichtshofs für Menschenrechte für die Auslegung und Anwendung der Konvention an¹⁶. Der Gerichtshof kann Entscheidungen über die Anwendung von Rechten im Zusammenhang mit Tätigkeiten öffentlicher Behörden in Brasilien erlassen, einschließlich Behörden, die Aufgaben im Bereich der öffentlichen Sicherheit und Verteidigung wahrnehmen¹⁷.

2.2. Der Datenschutzrahmen in Brasilien

- (11) Brasilien hat im Jahr 2018 ein allgemeines Gesetz im Bereich des Datenschutzes verabschiedet, das allen natürlichen Personen, unabhängig von ihrer

¹⁰ Artikel 25 der Verfassung der Föderativen Republik Brasilien von 1988.

¹¹ Verfassungsänderung Nr. 115 vom 10. Februar 2022. Abrufbar unter: http://www.planalto.gov.br/ccivil_03/Constituicao/Emendas/Emc/emc115.htm#art1.

¹² Siehe z. B. Artikel 4 Ziffer XIII des Gesetzes Nr. 13.445 vom 24. Mai 2017, Migrationsgesetz. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13445.htm#:~:text=Institui%20a%20Lei%20de%20Migra%C3%A7%C3%A3o.&text=Art.,pol%C3%ADticas%20p%C3%ABlicas%20para%20o%20emigrante.

¹³ Siehe z. B. FERREIRA FILHO, Manoel Gonçalves. Direitos humanos fundamentais. 6. ed. São Paulo: Saraiva, 2004.

¹⁴ Urteil des Superior Tribunal de Justiça, 4a Turma, 2016. Abrufbar unter: <https://www.jusbrasil.com.de/jurisprudencia/stj/863001318>.

¹⁵ Liste der Unterzeichnerstaaten und Ratifizierungen, Amerikanische Menschenrechtskonvention. Abrufbar unter: http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights_sign.htm.

¹⁶ Erklärung Brasiliens zur Konvention. Abrufbar unter: http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights_sign.htm#Brazil.

¹⁷ Siehe z. B. Urteil vom 6. Juli 2009 in der Rechtssache Escher et al./Brasilien. Abrufbar unter: https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_ing.pdf.

Staatsangehörigkeit, Schutz bietet: das allgemeine Datenschutzgesetz oder „Lei Geral de Proteção de Dados“ (im Folgenden „LGPD“)¹⁸.

- (12) Seit seiner Verabschiedung wurde das LGPD durch weitere Rechtsvorschriften gestärkt und präzisiert. Insbesondere wurde mit dem Gesetz Nr. 13.853 von 2019 die brasilianische Datenschutzbehörde (*Agência Nacional de Proteção de Dados – ANPD*)¹⁹ eingerichtet, die durch ein 2022 verabschiedetes Gesetz in eine unabhängige Behörde umgewandelt wurde²⁰. Dieses Gesetz wurde durch weitere verbindliche Erlasse ergänzt, unter anderem um den Status der ANPD aufzuwerten²¹ sowie ihre Zusammensetzung und das Verfahren zur Benennung ihrer Direktoren genauer festzulegen²².
- (13) Wie in den Erwägungsgründen 125 bis 141 dieses Beschlusses näher beschrieben, ist die ANPD die für die Auslegung und Durchsetzung des LGPD zuständige Behörde. In diesem Zusammenhang erlässt sie regelmäßig verbindliche Verordnungen zur Auslegung und Anwendung des Gesetzes. So hat sie beispielsweise mehrere Verordnungen verabschiedet, um die Sanktionsregelung weiterzuentwickeln und die Vorschriften für die Meldung von Verstößen gegen den Datenschutz zu präzisieren²³. Weitere Orientierungshilfen zur Anwendung und Auslegung des LGPD bietet die ANPD in Form von Dokumenten und Leitfäden, beispielsweise zur Auslegung der Rechtsgrundlage (z. B. berechtigtes Interesse) und der wichtigsten Begriffe im Rahmen des LGPD (z. B. Sanktionen, Datenschutzbeauftragter).
- (14) Im Rahmen ihres internationalen Engagements für die Förderung und den Schutz des Datenschutzes wurde die brasilianische ANPD 2023 neben allen Datenschutzbehörden der Europäischen Union Mitglied der Global Privacy Assembly²⁴. Brasilien trat zudem

¹⁸ Gesetz Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz. Abrufbar unter: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm und in englischer Sprache unter: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/lgpd-en-lei-no-13-709-capa.pdf>.

¹⁹ Gesetz Nr. 13.853 vom 8. Juli 2019 zur Änderung des LGPD, um unter anderem die Datenschutzbehörde – Autoridade Nacional de Proteção de Dados (ANPD) – zu schaffen. Abrufbar unter: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2.

²⁰ Gesetz Nr. 14.460 vom 25. Oktober 2022 zur Umwandlung der ANPD in eine Behörde mit Sonderstatus. Abrufbar unter: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm#art7.

²¹ Erlass Nr. 1.317 vom 17. September 2025 zur Änderung des LGPD zwecks Umgestaltung der ANPD. Abrufbar unter: <https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314>.

²² Erlass Nr. 10.474 vom 26. August 2020 zur Gründung der ANPD und zur Festlegung ihrer Zusammensetzung. Abrufbar unter: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226>. Erlass Nr. 11.758 vom 30. Oktober 2023 zur Änderung der Zusammensetzung der ANPD. Abrufbar unter: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11758.htm. Erlass vom 5. November 2020 über die Ernennung der Verwaltungsratsmitglieder der ANPD. Abrufbar unter: <https://www.in.gov.br/en/web/dou/-/decretos-de-5-de-novembro-de-2020-286734594>.

²³ Siehe Liste der Verordnungen der ANPD. Abrufbar unter: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes> und insbesondere die Verordnung Nr. 4 vom 24. Februar 2024 über die Anwendung von Verwaltungssanktionen. Abrufbar unter: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077> sowie Verordnung Nr. 15 vom 24. April 2024 über die Meldung von Verstößen gegen den Datenschutz. Abrufbar unter: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>.

²⁴ Die Global Privacy Assembly (GPA) ist ein Forum, das die Bemühungen von mehr als 130 Datenschutzbehörden aus der ganzen Welt vereint. Siehe die Ankündigung der ANPD anlässlich

dem Ausschuss des Europarats für das Übereinkommen Nr. 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten als Beobachter bei²⁵. Brasilien hat darüber hinaus bei mehreren Fortschritten, die bei den Vereinten Nationen (im Folgenden „VN“) in Bezug auf das Recht auf Privatsphäre erzielt wurden, eine Führungsrolle übernommen. Gemeinsam mit Deutschland brachte Brasilien die Resolutionen der Vereinten Nationen zum Recht auf Privatsphäre im digitalen Zeitalter ein, die 2013 und 2014 von der Generalversammlung der Vereinten Nationen verabschiedet wurden²⁶. Unter anderem heißt es in einer Resolution, dass „die unrechtmäßige oder willkürliche Überwachung und/oder die Überwachung der Kommunikation sowie die unrechtmäßige oder willkürliche Erhebung personenbezogener Daten als stark in die Privatsphäre eingreifende Handlungen gegen das Recht auf Privatsphäre und freie Meinungsäußerung verstoßen und den Grundsätzen einer demokratischen Gesellschaft zuwiderlaufen können“. Die Staaten werden aufgefordert, ihre Vorschriften zur Datenerhebung zu überprüfen, um sie mit den internationalen Menschenrechtsnormen in Einklang zu bringen, und „bestehende unabhängige, wirksame innerstaatliche Kontrollmechanismen einzurichten oder aufrechtzuerhalten, die in der Lage sind, gegebenenfalls Transparenz und Rechenschaftspflicht für die staatliche Überwachung der Kommunikation, ihre Erfassung und Aufzeichnung und die Erhebung personenbezogener Daten zu gewährleisten“²⁷.

- (15) Somit ist der brasilianische Rechtsrahmen für personenbezogene Daten, die gemäß diesem Beschluss übermittelt werden, seiner Struktur und seinen wesentlichen Bestandteilen nach dem in der Europäischen Union geltenden Rechtsrahmen sehr ähnlich. Dazu gehört auch, dass dieser Rechtsrahmen nicht nur auf Verpflichtungen beruht, die im innerstaatlichen Recht festgelegt sind und in der Verfassung garantiert werden, sondern auch auf völkerrechtlichen Verpflichtungen, die Brasilien insbesondere durch seinen Beitritt zur Amerikanischen Menschenrechtskonvention und durch die Anerkennung der Gerichtsbarkeit des Interamerikanischen Gerichtshofs für Menschenrechte eingegangen ist²⁸.

2.3. Sachlicher und räumlicher Geltungsbereich des LGPD

2.3.1. Räumlicher Geltungsbereich

- (16) Das LGPD gilt für jede Verarbeitung personenbezogener Daten in Brasilien, unabhängig davon, mit welchen Mitteln eine solche Tätigkeit ausgeübt wird²⁹.
- (17) In Artikel 3 LGPD wird der räumliche Geltungsbereich des Gesetzes festgelegt, der besagt, dass das Gesetz für die folgenden Tätigkeiten und unter den folgenden Bedingungen gilt: 1) Verarbeitungstätigkeiten, die im Hoheitsgebiet Brasiliens (das die Union, die Bundesstaaten, den Bundesdistrikt sowie die Gemeinden umfasst)

ihres Beitritts zur GDA. Abrufbar unter: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-aceita-como-membro-pleno-no-global-privacy-assembly>.

²⁵ Europarat, Beobachter im Ausschuss für das Übereinkommen Nr. 108. Abrufbar unter: <https://rm.coe.int/list-of-observers-december-2022-bilingual-2781-7012-1734-1/1680a962eb>.

²⁶ Siehe beispielsweise die Resolution der Generalversammlung der Vereinten Nationen über das Recht auf Privatsphäre im digitalen Zeitalter vom 18. Dezember 2013. Abrufbar unter: <https://digitallibrary.un.org/record/764407?ln=en&v=pdf>.

²⁷ Generalversammlung der Vereinten Nationen, Resolution über das Recht auf Privatsphäre im digitalen Zeitalter, 18. Dezember 2013, S. 1-2.

²⁸ Siehe Interamerikanischer Gerichtshof für Menschenrechte. Fragen und Antworten zur Zuständigkeit des Gerichtshofs. Abrufbar unter: https://www.corteidh.or.cr/que_es_la_corte.cfm?lang=en.

²⁹ Artikel 3 des Gesetzes Nr. 13.709/14 vom August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

durchgeführt werden, 2) Verarbeitungstätigkeiten, die dazu dienen, Waren oder Dienstleistungen anzubieten oder zu liefern, oder die Verarbeitung von Daten natürlicher Personen, die sich im Hoheitsgebiet Brasiliens aufhalten, 3) wenn die verarbeiteten personenbezogenen Daten im Hoheitsgebiet Brasiliens erhoben wurden. Dieser Ansatz gleicht dem Ansatz, der mit Artikel 3 der Verordnung (EU) 2016/679 verfolgt wird.

- (18) Darüber hinaus fällt nach Artikel 3 Ziffer II LGPD jede Verarbeitung personenbezogener Daten von natürlichen Personen, die sich im Hoheitsgebiet Brasiliens aufhalten, unter das Gesetz. Dies schließt die Verarbeitung von Daten zur Überwachung des Verhaltens von natürlichen Personen im Hoheitsgebiet ein, unabhängig davon, wo die Daten verarbeitet werden.
- (19) Schließlich folgt aus der Rechtsprechung des Obersten Bundesgerichts (Supremo Tribunal Federal), dass die durch die Verfassung garantierten Grundrechte, wie das Recht auf Datenschutz, für jede Person gelten, unabhängig von der Staatsangehörigkeit oder dem Wohnsitz der betroffenen Person³⁰.

2.3.2. Definition des Begriffs „personenbezogene Daten“

- (20) In Artikel 5 Ziffer I LGPD werden personenbezogene Daten als Informationen definiert, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Nach dem Gesetz ist eine „betroffene Person“ eine „natürliche Person, auf die sich die verarbeiteten personenbezogenen Daten beziehen“³¹.
- (21) Darüber hinaus gelten pseudonymisierte Informationen – d. h. Informationen, anhand derer eine bestimmte natürliche Person nicht mehr unmittelbar oder indirekt identifiziert werden kann oder die ohne zusätzliche Informationen zur Wiederherstellung des ursprünglichen Zustands zu verwenden/kombinieren, nicht mehr mit ihr in Verbindung gebracht werden können – als personenbezogene Daten nach dem LGPD³².
- (22) Umgekehrt sind Daten, die vollständig „anonymisiert“ sind, vom Anwendungsbereich des LGPD ausgenommen³³. Nach Artikel 5 LGPD sind anonymisierte Daten als Daten definiert, die unter Verwendung angemessener und technischer Mittel, die zum Zeitpunkt der Verarbeitung zur Verfügung stehen, nicht unmittelbar oder indirekt mit einer natürlichen Person in Verbindung gebracht werden können. In Artikel 12 LGPD wird näher ausgeführt, dass anonymisierte Daten nicht als personenbezogene Daten gelten, es sei denn, der Prozess der Anonymisierung, dem die Daten unterzogen wurden, wurde rückgängig gemacht oder kann mit „angemessenem Aufwand“ rückgängig gemacht werden. In Artikel 12 LGPD wird zudem betont, dass bei der Bestimmung dessen, was als „angemessen“ gilt, objektive Faktoren berücksichtigt werden müssen, wie z. B.: 1) Kosten und Zeit, die erforderlich sind, um die Anonymisierung wieder rückgängig zu machen, 2) die verfügbare Technologie und 3) die ausschließliche Nutzung eigener Mittel eines Verantwortlichen. Der Ansatz für die

³⁰ Entscheidung des Superior Tribunal de Justiça, 4a Turma, 2016. Abrufbar unter: <https://www.jusbrasil.com.de/jurisprudencia/stj/863001318>.

³¹ Artikel 5 Ziffer V des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

³² Artikel 13 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

³³ Artikel 12 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

Anonymisierung und die im LGPD eingeführten Schutzmaßnahmen, um eine erneute Identifizierung zu verhindern, sind ähnlich wie in der EU.

- (23) Dies entspricht dem sachlichen Geltungsbereich der Verordnung (EU) 2016/679 und den darin genannten Definitionen der Begriffe „personenbezogene Daten“, „Pseudonymisierung“ und „anonymisierte Daten“.

2.3.3. **Die Definition des Begriffs „Verarbeitung“**

- (24) Die Definitionen des Begriffs „Verarbeitung“ in den Systemen der Europäischen Union und Brasiliens beziehen sich beide auf „jeden Vorgang“, der im Zusammenhang mit personenbezogenen Daten durchgeführt wird³⁴. Artikel 5 Ziffer X LGPD enthält die folgende nicht erschöpfende Liste von Tätigkeiten, bei denen es sich um eine Verarbeitung handelt: „Erhebung, Herstellung, Empfang, Einstufung, Verwendung, Zugriff, Vervielfältigung, Übermittlung, Verbreitung, Verarbeitung, Archivierung, Speicherung, Löschung, Auswertung oder Kontrolle von Informationen, Änderungen, Kommunikation, Übertragung, Verbreitung oder Extraktion“.

2.3.4. Verantwortlicher und Auftragsverarbeiter

- (25) Der Begriff des Verantwortlichen ist im LGPD definiert als die natürliche oder juristische Person des öffentlichen oder privaten Rechts, die für Entscheidungen über die Verarbeitung personenbezogener Daten verantwortlich ist³⁵.
- (26) Der Begriff des Auftragsverarbeiters ist im LGPD definiert als die natürliche oder juristische Person des öffentlichen oder privaten Rechts, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet³⁶. Der Auftragsverarbeiter muss die Verarbeitung gemäß den Anweisungen des Verantwortlichen durchführen, der für die Überprüfung der Einhaltung der Vorschriften verantwortlich ist³⁷.
- (27) Der Verantwortliche und der Auftragsverarbeiter müssen Aufzeichnungen über die von ihnen durchgeführten Verarbeitungen personenbezogener Daten führen, insbesondere wenn diese auf einem berechtigten Interesse beruhen³⁸.
- (28) Nach dem LGPD haften zwei oder mehr Verantwortliche, die unmittelbar an der Verarbeitung beteiligt sind, durch die die betroffene Person einen Schaden erlitten hat, gesamtschuldnerisch³⁹. Ein Auftragsverarbeiter haftet gesamtschuldnerisch für den durch die Verarbeitung verursachten Schaden, wenn er den Verpflichtungen gemäß Artikel 44 LGPD nicht nachkommt oder wenn er die rechtlichen Anweisungen des Verantwortlichen nicht befolgt hat⁴⁰.

³⁴ Artikel 5 Ziffer X des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

³⁵ Artikel 5 Ziffer VI des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

³⁶ Artikel 5 Absatz VII des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

³⁷ Artikel 39 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

³⁸ Artikel 37 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

³⁹ Artikel 42 Absatz 1 Ziffer II des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁴⁰ Artikel 42 Absatz 1 Ziffer I des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

- (29) Daher sind die Vorschriften zur Regelung der Beziehung zwischen Verantwortlichen und Auftragsverarbeitern im Rahmen des LGPD ähnlich wie die Vorschriften in Kapitel IV der Verordnung (EU) 2016/679.

2.3.5. Ausnahme von einigen Bestimmungen des LGPD

- (30) Wie im System der Europäischen Union gilt das LGPD nicht für anonymisierte Daten⁴¹, für die Verarbeitung personenbezogener Daten zu rein privaten Zwecken⁴² oder wenn diese ausschließlich zum Zwecke der öffentlichen Sicherheit, der Landesverteidigung, der Staatssicherheit oder der Untersuchung und Verfolgung von Straftaten erfolgt⁴³.
- (31) Die Ausnahme im Bereich der öffentlichen Sicherheit, der Landesverteidigung, der Staatssicherheit sowie der Untersuchung und Verfolgung von Straftaten gilt jedoch nur teilweise. Das Oberste Bundesgericht hat die Anwendbarkeit des LGPD im Lichte des verfassungsmäßigen Schutzes personenbezogener Daten ausgelegt und festgestellt, dass die wichtigsten Grundsätze, Rechte und Ziele des LGPD für jede Verarbeitung personenbezogener Daten durch Behörden gelten, auch wenn sie für „nachrichtendienstliche“ Zwecke erfolgt⁴⁴. Ferner sind in Artikel 4 Absätze 2 bis 4 LGPD die Bedingungen für die Verarbeitung personenbezogener Daten zum Zwecke der öffentlichen Sicherheit, der Landesverteidigung, der Staatssicherheit oder der Untersuchung und Verfolgung von Straftaten festgelegt, insbesondere um private Einrichtungen daran zu hindern, Daten für solche Zwecke zu verarbeiten, die ANPD anzuweisen, technische Gutachten und Empfehlungen zu diesem Thema abzugeben, und die ANPD zu ermächtigen, eine Datenschutz-Folgenabschätzung in Bezug auf diese Tätigkeiten anzufordern⁴⁵. Auf dieser Grundlage hat die ANPD beispielsweise Untersuchungen durchgeführt und Leitlinien herausgegeben, wie einen an das Ministerium für Justiz und öffentliche Sicherheit gerichteten technischen Vermerk über den Einsatz von Technologien, einschließlich Gesichtserkennung, im öffentlichen Raum⁴⁶. In diesem Vermerk wies die ANPD darauf hin, dass die Verarbeitung für diese Zwecke mit den allgemeinen Grundsätzen und Rechten des LGPD vereinbar sein muss⁴⁷.
- (32) Artikel 4 Ziffer II LGPD sieht ferner eine teilweise Ausnahmeregelung für die Verarbeitung personenbezogener Daten für Zwecke der akademischen Forschung sowie für journalistische und künstlerische Zwecke vor.
- (33) In Bezug auf die akademische Forschung ist die Ausnahmeregelung durch mehrere Faktoren beschränkt. Erstens muss die Verarbeitung nach Artikel 4 Ziffer II LGPD

⁴¹ Artikel 12 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁴² Artikel 4 Ziffer I des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁴³ Artikel 4 Ziffer III des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁴⁴ Oberstes Bundesgericht. Entscheidung in der Rechtssache ADI 6649, September 2022. Abrufbar unter: <https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false>.

⁴⁵ Artikel 4 Absätze 2-4 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁴⁶ Technischer Vermerk Nr. 175/2023 zum Entwurf eines Kooperationsabkommens zwischen dem Ministerium für Justiz und öffentliche Sicherheit und dem brasilianischen Fußballverband über den Austausch personenbezogener Daten im Hinblick auf die Verbesserung des Projekts „Sichere Stadien“. Abrufbar unter: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mjsp-e-cbf.pdf>.

⁴⁷ Technischer Vermerk Nr. 175/2023, Absatz 5.1.

„ausschließlich“ zu Zwecken der akademischen Forschung erfolgen. Zweitens ist in Artikel 4 Ziffer II Buchstabe b LGPD festgelegt, dass Artikel 7 (Erfordernis einer Rechtsgrundlage) und Artikel 11 (Vorschriften über die Verarbeitung sensibler Daten) für diese Art der Verarbeitung gelten⁴⁸. Drittens hat die ANPD einen Leitfaden erarbeitet, um die Vorschriften für die Verarbeitung von Daten zu akademischen und Forschungszwecken näher zu erläutern, unter anderem indem genau festgelegt wird, welche Einrichtungen als „Forschungseinrichtung“ im Sinne des Artikels 5 Ziffer XVII LGPD angesehen werden können⁴⁹. In diesem Leitfaden bestätigt die ANPD, dass die Verarbeitung von Daten zu Zwecken der akademischen Forschung nur teilweise vom LGPD ausgenommen ist und die allgemeinen Grundsätze des Gesetzes Anwendung finden⁵⁰.

- (34) In Bezug auf Daten, die speziell für die Gesundheitsforschung verwendet werden, enthält das LGPD zusätzliche Einschränkungen. Zum einen legt Artikel 13 LGPD Sicherheitspflichten für die verwendeten Datenbanken fest und fördert den Einsatz von Anonymisierungs- und Pseudonymisierungstechniken. Es sieht ferner vor, dass Forschungseinrichtungen für die Nichtumsetzung von Sicherheitsmaßnahmen zum Schutz personenbezogener Daten haftbar gemacht werden können⁵¹. Andererseits ist die Weitergabe von Daten, die für die Gesundheitsforschung verwendet werden, an Dritte „unter keinen Umständen“ zulässig⁵².
- (35) In Bezug auf die Verarbeitung personenbezogener Daten zu journalistischen und künstlerischen Zwecken ähnelt die Ausnahme des LGPD der in Artikel 85 Absatz 2 der Verordnung (EU) 2016/679 vorgesehenen Ausnahme. Die Ausnahme gemäß LGPD gilt für Fälle, in denen die Verarbeitung „ausschließlich“ zu diesen Zwecken erfolgt⁵³. Das bedeutet, dass das LGPD in vollem Umfang gilt, wenn Presse-, Medien- und Kunstorganisationen personenbezogene Daten zu anderen Zwecken, z. B. für die Personalverwaltung oder die interne Verwaltung, verarbeiten.
- (36) Künstlerische Meinungsäußerung und Medienfreiheit sind beide Teil des Rechts auf freie Meinungsäußerung gemäß Artikel 5 Ziffer IX der Verfassung, der die freie Meinungsäußerung für „intellektuelle, künstlerische, wissenschaftliche und kommunikative“ Äußerungen garantiert. Hinsichtlich der Abwägung zwischen dem Recht auf freie Meinungsäußerung und anderen Rechten (einschließlich des Rechts auf Privatsphäre und Datenschutz) gelten die in der Verfassung festgelegten Kriterien in der Auslegung durch das Oberste Bundesgericht. Insbesondere erfordert die Ausübung des Rechts auf freie Meinungsäußerung keine vorherige Genehmigung, sondern unterliegt weiterhin den Beschränkungen, die für den Schutz anderer Grundrechte

⁴⁸ Artikel 4 Ziffer II Buchstabe b des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁴⁹ Leitfaden der ANPD zur Verarbeitung personenbezogener Daten zu akademischen Zwecken und zur Durchführung von Forschungsarbeiten, Juni 2023. Abrufbar unter: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf>.

⁵⁰ Siehe insbesondere S. 18 bis 43 des Leitfadens zur Verarbeitung personenbezogener Daten zu akademischen Zwecken und zur Durchführung von Forschungsarbeiten.

⁵¹ Artikel 13 Absatz 2 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁵² Artikel 13 Absatz 2 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz. Leitfaden der ANPD zur Verarbeitung personenbezogener Daten zu akademischen Zwecken und zur Durchführung von Forschungsarbeiten, Juni 2023, S. 15.

⁵³ Artikel 4 Ziffer II Buchstabe a des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

gelten. Insbesondere kann eine natürliche Person im Falle eines Schadens oder einer Verletzung des Rechts auf Privatsphäre gemäß Artikel 5 Ziffer X der Verfassung Schadenersatz verlangen. Darüber hinaus wurden diese Garantien in das Zivilrechtliche Rahmenwerk für das Internet aufgenommen, ein Gesetz, das im Jahr 2014 zum Schutz der Grundrechte im Internet verabschiedet wurde⁵⁴. Insbesondere Artikel 7 Ziffer I des Zivilrechtlichen Rahmenwerks für das Internet garantiert die „Unverletzlichkeit der Privatsphäre“ und begründet einen Anspruch auf Entschädigung für materielle oder immaterielle Schäden, die sich aus einer Verletzung der Privatsphäre ergeben. Darüber hinaus verweist das Oberste Bundesgericht in seiner Rechtsprechung auf die Notwendigkeit, „ein Gleichgewicht zwischen den Rechten herzustellen und das Recht auf freie Meinungsäußerung mit der Unverletzlichkeit der Privatsphäre in Einklang zu bringen“, und betont, wie wichtig das Recht auf Rechtsbehelfe und der Zugang zu Rechtsbehelfen im Falle einer Verletzung der Privatsphäre ist⁵⁵. In einem anderen Fall wies das Oberste Bundesgericht darauf hin, dass „die Pressefreiheit und die Freiheit der sozialen Kommunikation im Einklang mit anderen Verfassungsgrundsätzen“ wie der Unverletzlichkeit der Privatsphäre und dem Recht auf Datenschutz ausgeübt werden müssen⁵⁶.

- (37) Schließlich ist nach dem LGPD die Verarbeitung von Daten, die ihren Ursprung außerhalb Brasiliens haben und entweder 1) nicht an Verarbeitungsagenten in Brasilien weitergegeben oder übermittelt werden oder 2) aus einem Land stammen, das nach dem LGPD als angemessen eingestuft wurde, vom Geltungsbereich des Gesetzes ausgenommen, sofern die Daten nicht in ein anderes Land übermittelt werden⁵⁷. Die ANPD hat eine verbindliche Auslegung vorgenommen, um die beiden Szenarien in ihrer Datenübermittlungsverordnung eindeutig zu klären⁵⁸.
- (38) Im ersten Szenario wäre die bloße Übermittlung personenbezogener Daten durch Brasilien ohne zusätzliche Verarbeitung im Land vom Geltungsbereich des Gesetzes ausgenommen⁵⁹. Sobald jedoch in Brasilien auf Daten zugegriffen, Daten verwendet oder anderweitig verarbeitet würden, würde das LGPD gelten. Die bestehenden innerstaatlichen Vorschriften über die Cybersicherheit und zum Zugriff auf Daten durch Behörden würden auch in diesem begrenzten Szenario weiterhin gelten, unabhängig davon, ob die Daten verarbeitet werden oder sich nur im Transit befinden.
- (39) Im zweiten Szenario stellt die ANPD klar, dass nur die Rückübertragung von Daten, die ursprünglich aus einem Land übermittelt wurden, für das ein Angemessenheitsbeschluss nach dem LGPD gilt, vom Gesetz ausgenommen ist, sofern für diese Verarbeitung das nationale Recht dieses angemessenen Landes gilt. Auch in diesem Fall würden die Vorschriften über die Cybersicherheit und zum Zugriff auf Daten durch Behörden weiterhin gelten. Im Zusammenhang mit der

⁵⁴ Gesetz Nr. 12.965 vom 23. April 2014, Marco Civil da Internet („Zivilrechtliches Rahmenwerk für das Internet“). Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

⁵⁵ Oberstes Bundesgericht, Entscheidung in der Rechtssache ADI 4815. Abrufbar unter: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4271057>.

⁵⁶ Oberstes Bundesgericht, Entscheidung in der Rechtssache ADI 5418. Abrufbar unter: <https://www.jurisprudencia.stf.jus.br/pages/search/sjur446943/false>.

⁵⁷ Artikel 4 Ziffer IV des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁵⁸ Anhang I Abschnitt III, ANPD, Verordnung über die internationale Übermittlung personenbezogener Daten (im Folgenden „Datenübermittlungsverordnung“). Abrufbar unter: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulation-on-international-transfer-of-personal-data.pdf>.

⁵⁹ Artikel 8 Ziffer I, ANPD, Verordnung über die internationale Übermittlung personenbezogener Daten.

Übermittlung personenbezogener Daten zwischen der EU und Brasilien würde, falls die EU von einem Angemessenheitsbeschluss aus Brasilien profitieren würde, die Übermittlung von Daten aus Brasilien in die EU nicht immer in den Anwendungsbereich des Artikels 3 der Verordnung (EU) 2016/679 fallen. Daher ergibt sich aus Artikel 8 Ziffer II Buchstabe b der Datenübermittlungsverordnung, dass in Fällen, in denen die in Frage stehende Verarbeitung nicht in den Anwendungsbereich der Verordnung (EU) 2016/679 fällt, das LGPD für die Rückübertragung von Daten aus Brasilien in die EU gelten würde.

2.4. Garantien, Rechte und Pflichten

2.4.1. Rechtmäßigkeit der Verarbeitung und Verarbeitung nach Treu und Glauben

- (40) Die Verarbeitung personenbezogener Daten sollte rechtmäßig und nach Treu und Glauben erfolgen.
- (41) Die Grundsätze der Rechtmäßigkeit, des guten Glaubens und der Transparenz sowie die Gründe für die rechtmäßige Verarbeitung sind in den Artikeln 6 und 7 LGPD durch Bedingungen gewährleistet, die den Artikeln 5 und 6 der Verordnung (EU) 2016/679 ähneln.
- (42) Gemäß den Artikeln 6 und 7 LGPD müssen die Verantwortlichen und Auftragsverarbeiter personenbezogene Daten rechtmäßig und nach Treu und Glauben in dem für den angegebenen Zweck erforderlichen Mindestumfang verarbeiten, wobei die Verarbeitung sich auf Daten beschränken muss, die für den Zweck relevant, verhältnismäßig und nicht übermäßig sind⁶⁰.
- (43) Diese allgemeinen Grundsätze der rechtmäßigen Datenverarbeitung werden in Artikel 7 LGPD näher erläutert, wo die verschiedenen Rechtsgrundlagen für die Verarbeitung, einschließlich der Umstände, unter denen diese eine Änderung des Zwecks beinhalten können, dargelegt sind.
- (44) Gemäß Artikel 7 LGPD dürfen ein Verantwortlicher und ein Auftragsverarbeiter personenbezogene Daten nur aufgrund einer begrenzten Anzahl von Rechtsgrundlagen verarbeiten. Im LGPD sind folgende Rechtsgrundlagen vorgesehen: 1) die Einwilligung der betroffenen Person (Ziffer I), 2) die Notwendigkeit, einen Vertrag oder eine vorvertragliche Maßnahme im Zusammenhang mit einem Vertrag, dessen Vertragspartei die betroffene Person ist, auf Antrag der betroffenen Person auszuführen (Ziffer V), 3) die Einhaltung einer rechtlichen oder regulatorischen Verpflichtung durch den Verantwortlichen⁶¹ (Ziffer II), 4) zum Schutz des Lebens oder der körperlichen Unversehrtheit der betroffenen Person oder eines Dritten (Ziffer VII), 5) die Verarbeitung von Daten durch eine öffentliche Verwaltung, die für die Durchführung öffentlicher Maßnahmen erforderlich ist, die in Gesetzen und sonstigen Vorschriften vorgesehen sind, oder auf der Grundlage von Verträgen, Vereinbarungen oder ähnlichen Instrumenten⁶² (Ziffer III) und 6), wenn dies zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten erforderlich ist, außer in Fällen, in denen die Grundrechte und

⁶⁰ Siehe insbesondere Artikel 6, Hauptabsatz, Ziffern III, I und V sowie Artikel 7 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁶¹ Jede rechtliche oder regulatorische Verpflichtung muss gesetzlich festgelegt sowie notwendig und verhältnismäßig sein.

⁶² Die besonderen Bestimmungen für die Verarbeitung personenbezogener Daten durch Behörden gemäß Kapitel IV des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), sind einzuhalten.

Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, Vorrang haben (Ziffer IX).

- (45) Artikel 7 LGPD sieht vier zusätzliche spezifische Rechtsgrundlagen für die Verarbeitung von Daten vor: 1) zur Durchführung von Studien durch Forschungseinrichtungen, wobei nach Möglichkeit die Anonymisierung personenbezogener Daten sicherzustellen ist (Ziffer IV), 2) zur regelmäßigen Ausübung von Rechten in Gerichts-, Verwaltungs- oder Schiedsverfahren⁶³ (Ziffer VI), 3) zum Schutz der Gesundheit, ausschließlich in einem Verfahren, das von Angehörigen der Gesundheitsberufe, Gesundheitsdienste oder Gesundheitsbehörden durchgeführt wird (Ziffer VIII) und 4) zur Kreditsicherung (Ziffer X)⁶⁴.

2.4.2. Kriterien für die Einwilligung

- (46) Die formalen Anforderungen an die Einholung einer gültigen Einwilligung zur Verarbeitung personenbezogener Daten gemäß LGPD sind in Artikel 8 festgelegt und folgen einem ähnlichen Ansatz wie Artikel 4 Absatz 11 und Artikel 7 der Verordnung (EU) 2016/679. Erstens muss die Einwilligung entweder schriftlich oder auf anderem Wege erteilt werden, wodurch die „Willensbekundung“ der betroffenen Person nachgewiesen werden kann⁶⁵. In ihren Leitlinien stellt die ANPD klar, dass „die Einwilligung eindeutig sein muss, was voraussetzt, dass die betroffene Person ihren Willen eindeutig und positiv zum Ausdruck bringt“, und was bedeutet, dass es nicht zulässig ist, die Einwilligung „auf stillschweigende Weise oder durch Unterlassung der betroffenen Person“⁶⁶ einzuholen. Zweitens muss sich die Einwilligung auf „bestimmte Zwecke“ beziehen, und „allgemeine Zustimmungen zur Verarbeitung“ personenbezogener Daten gelten als nichtig⁶⁷. Drittens muss die Einwilligung auf der Grundlage von Informationen erfolgen, die „transparent, klar und eindeutig“ bereitgestellt werden⁶⁸. Wird die Einwilligung in einen umfassenderen Vertrag aufgenommen, so muss sie in einer gesonderten und spezifischen Klausel erscheinen,

⁶³ Die Verfahren sind im Gesetz Nr. 9.307 vom 23. September 1996 über die Schiedsgerichtsbarkeit beschrieben.

⁶⁴ Im Hinblick auf die Kreditsicherung hat die Aufnahme dieser Rechtsgrundlagen in das LGPD das Schutzniveau für betroffene Personen erhöht, indem beispielsweise sichergestellt wurde, dass Kreditinstitute nur die für die Kreditanalyse und -rückforderung erforderlichen personenbezogenen Daten verarbeiten. Seit der Verabschiedung des LGPD haben die brasilianischen Gerichte mehrere Entscheidungen erlassen, um beispielsweise die Verarbeitung von Daten zum Zwecke der Kreditsicherung einzuschränken, indem sie Daten wie „Wählerregistrierungsnummer, Name der Mutter, Lebensstil, soziale Schicht, Schulbildung, marginaler Konsumhang und Georeferenzierung“, die nicht für notwendig erachtet wurden, ausgeschlossen haben. Die Gerichte haben ferner klargestellt, dass ein weiterer Zugriff auf personenbezogene Daten die Einwilligung der betroffenen Person erfordern würde, wodurch der Umfang der Datenverarbeitung zum Zwecke der Kreditsicherung eingeschränkt wird. Siehe Opice Blum Advogados, Jurimetrics Report, 2022. Abrufbar unter: <https://opiceblum.com.br/wp-content/uploads/2019/07/09-relatorio-jurimetria-2022.pdf>.

⁶⁵ Artikel 8, Hauptabsatz des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁶⁶ ANPD, Leitfaden zu Cookies und Datenschutz, S. 18-19. Abrufbar unter: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf>.

⁶⁷ Artikel 8 Absatz 4 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz. Darüber hinaus ist für die Weitergabe personenbezogener Daten zwischen Verantwortlichen eine gesonderte, spezifische Einwilligung erforderlich, es sei denn, die Daten wurden gemäß Artikel 7 Absatz 5 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz offensichtlich öffentlich zugänglich gemacht.

⁶⁸ Artikel 9 Absatz 1 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

die sich deutlich von den anderen Vertragsbestimmungen abhebt⁶⁹. Darüber hinaus gilt die Einwilligung als ungültig, wenn die der betroffenen Person zur Verfügung gestellten Informationen „irreführende oder missbräuchliche Inhalte“ enthalten⁷⁰. Der für die Verarbeitung Verantwortliche muss die betroffene Person auch über jede Änderung in Bezug auf Folgendes in Kenntnis setzen: 1) den bestimmten Zweck der Verarbeitung, 2) Art und Dauer der Verarbeitung, 3) die Identität des Verantwortlichen oder 4) alle Informationen über die Verarbeitung und mögliche Weitergabe von Daten⁷¹. Viertens muss die Einwilligung von der betroffenen Person im Rahmen eines „kostenlosen Verfahrens“ „jederzeit widerrufen“ werden können⁷².

- (47) Das LGPD enthält ein strenges Verbot der Verarbeitung personenbezogener Daten, wenn die Einwilligung fehlerhaft oder ungültig ist⁷³. Im LGPD wird ferner klargestellt, dass der Verantwortliche die Beweislast dafür trägt, dass die Einwilligung im Einklang mit dem LGPD rechtmäßig eingeholt wurde⁷⁴.
- (48) Schließlich ist im LGPD festgelegt, dass in Fällen, in denen die Einwilligung die geeignete Rechtsgrundlage für die Verarbeitung wäre, von der Einwilligungspflicht abgesehen wird, wenn personenbezogene Daten von der betroffenen Person „offensichtlich öffentlich“ gemacht wurden⁷⁵. Der Begriff „offensichtlich öffentliche Daten“ findet sich auch in Artikel 9 der Verordnung (EU) 2016/679. Doch auch wenn von der Einwilligungspflicht abgesehen wird, sind Verantwortliche und Auftragsverarbeiter nicht von der Einhaltung aller anderen im LGPD festgelegten Rechte und Pflichten befreit⁷⁶. Insbesondere dürfen Daten, die von der betroffenen Person offensichtlich öffentlich gemacht wurden, weiterverarbeitet werden, sofern dies zu einem „berechtigten und bestimmten“ Zweck geschieht und die Rechte der betroffenen Personen und die im LGPD festgelegten Grundsätze eingehalten werden⁷⁷.

2.4.3. Kriterien für ein berechtigtes Interesse

- (49) In Artikel 7 Ziffer IX LGPD ist festgelegt, dass die Verarbeitung personenbezogener Daten niemals aus Gründen des berechtigten Interesses erfolgen darf, wenn eine solche Verarbeitung den Grundrechten und Grundfreiheiten der betroffenen Personen zuwiderlaufen würde, und es wird betont, dass der Schutz personenbezogener Daten Vorrang hat. Dieser Ansatz ähnelt dem Ansatz, der in der EU verfolgt und in Artikel 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 dargelegt wird.

⁶⁹ Artikel 8 Absatz 1 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁷⁰ Artikel 9 Absatz 1 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁷¹ Artikel 8 Absatz 6 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁷² Artikel 8 Absatz 5 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁷³ Artikel 8 Absatz 3 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁷⁴ Artikel 8 Absatz 2 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁷⁵ Artikel 7 Absatz 4 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz. Der Anwendungsbereich dieser Maßnahme ist begrenzt, da sie nicht die nach Artikel 9 Absatz 2 Buchstabe e der Verordnung (EU) 2016/679 zulässige Verarbeitung sensibler Daten umfasst.

⁷⁶ Artikel 7 Absatz 4 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁷⁷ Artikel 7 Absatz 7 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

- (50) In Artikel 10 LGPD sind die zusätzlichen Bedingungen festgelegt, unter denen sich die Verantwortlichen auf ein „berechtigtes Interesse“ als Rechtsgrundlage für die Verarbeitung personenbezogener Daten berufen können. Erstens darf der Verantwortliche, wenn die Verarbeitung personenbezogener Daten auf einem berechtigten Interesse beruht, nur personenbezogene Daten verarbeiten, die für den beabsichtigten Zweck „unbedingt erforderlich“ sind⁷⁸. Zweitens muss der Verantwortliche auch Maßnahmen ergreifen, um die Transparenz der Verarbeitungstätigkeit zu gewährleisten⁷⁹. Drittens kann ein berechtigtes Interesse nur in „besonderen Situationen“ geltend gemacht werden⁸⁰.
- (51) Darüber hinaus hat die ANPD den „Leitfaden zum berechtigten Interesse“ veröffentlicht, in dem die Bedingungen für die Geltendmachung des berechtigten Interesses ausführlich dargelegt sind⁸¹. In diesem Leitfaden wird beispielsweise klargestellt, dass ein berechtigtes Interesse nicht als Rechtsgrundlage für die Verarbeitung sensibler Daten herangezogen werden kann⁸², und der Anhang enthält ein Modell für die Abwägungsprüfung zum Schutz der Grundrechte und Grundfreiheiten, das alle Verantwortlichen, die sich auf ein berechtigtes Interesse berufen möchten, verwenden können⁸³. Ferner kann die ANPD von dem Verantwortlichen die Durchführung einer Datenschutz-Folgenabschätzung verlangen⁸⁴.
- (52) Im Leitfaden stellt die ANPD klar, dass ein Interesse nur dann als „berechtigt“ gelten kann, wenn drei Voraussetzungen erfüllt sind: 1) Vereinbarkeit mit der brasilianischen Rechtsordnung, 2) Bezugnahme auf einen bestimmten Fall und 3) die Verarbeitung muss mit berechtigten, spezifischen und eindeutigen Zwecken verknüpft sein⁸⁵. Die erste Voraussetzung „Vereinbarkeit mit der Rechtsordnung“ besagt, dass das vom Verantwortlichen geltend gemachte berechtigte Interesse mit den in Brasilien garantierten Grundsätzen, Rechtsnormen und Grundrechten vereinbar sein muss. Dies bedeutet beispielsweise, dass die beabsichtigte Verarbeitung personenbezogener Daten nicht durch eine brasilianische Rechtsvorschrift verboten sein darf und weder direkt noch indirekt im Widerspruch zu Rechtsvorschriften oder Grundsätzen des brasilianischen Rechts stehen darf. Zweitens muss das geltend gemachte berechtigte Interesse auf „konkreten, eindeutigen und klaren“ Situationen beruhen, die auf spezifische und genau umrissene Interessen abzielen. Das geltend gemachte

⁷⁸ Artikel 10 Absatz 1 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁷⁹ Artikel 10 Absatz 2 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁸⁰ Artikel 10 LGPD enthält einige Beispiele für besondere Situationen, in denen ein berechtigtes Interesse geltend gemacht werden kann: 1) Unterstützung und Förderung der Tätigkeiten des Verantwortlichen (Ziffer I), 2) Schutz der Ausübung der Rechte der betroffenen Person oder Ermöglichung der Erbringung von Dienstleistungen, die der betroffenen Person zugutekommen, sofern bei dieser Verarbeitung die berechtigten Erwartungen, Grundrechte und Grundfreiheiten der betroffenen Person gewahrt werden (Ziffer II). Gesetz Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁸¹ ANPD, Leitfaden – Rechtsgrundlagen für die Verarbeitung personenbezogener Daten – Berechtigtes Interesse, Februar 2024 („Leitfaden zum berechtigten Interesse“). Abrufbar unter: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf.

⁸² ANPD, Leitfaden zum berechtigten Interesse, S. 8.

⁸³ ANPD, Leitfaden zum berechtigten Interesse, Anhang 3.

⁸⁴ Artikel 10 Absatz 3 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁸⁵ ANPD, Leitfaden zum berechtigten Interesse, S. 16-17.

berechtigte Interesse kann nicht auf „abstrakte oder rein spekulative Situationen“ gestützt werden⁸⁶. Die ANPD führt ferner aus, dass Interessen, die nicht mit den „aktuellen Tätigkeiten des Verantwortlichen in Verbindung stehen, nicht als berechtigt angesehen werden“⁸⁷. Die dritte Voraussetzung bezieht sich auf die Notwendigkeit, einen bestimmten Zweck der Verarbeitung nachzuweisen. Die ANPD weist darauf hin, dass das berechtigte Interesse des Verantwortlichen (das die Verarbeitung rechtfertigt) nicht mit dem Zweck der Verarbeitung verwechselt werden darf (der den spezifischen Zweck darstellt, der durch die Durchführung der Verarbeitung erreicht werden soll). Das Vorliegen eines berechtigten Interesses entbindet den Verantwortlichen nicht von der Verpflichtung, den Grundsatz der Zweckbindung und alle Verpflichtungen aus dem LGPD einzuhalten. Der Zweck muss klar und genau beschrieben werden und die Informationen umfassen, die erforderlich sind, um den Umfang der Verarbeitung abzugrenzen und eine Abwägung der Interessen des Verantwortlichen oder Dritter mit den Rechten und berechtigten Erwartungen der betroffenen Personen zu ermöglichen⁸⁸. Dies bedeutet, dass ein Verantwortlicher, wenn er sich auf ein berechtigtes Interesse zur Unterstützung oder Förderung seiner Tätigkeit beruft, unter anderem klar definieren muss, welche Tätigkeit er zu fördern/zu unterstützen beabsichtigt und in welchem Zusammenhang dies mit der beabsichtigten Verarbeitung steht.

2.4.4. Verarbeitung besonderer Datenkategorien

- (53) Wenn besondere Kategorien von Daten verarbeitet werden, sollte es besondere Garantien geben.
- (54) In Artikel 5 Ziffer II LGPD werden sensible personenbezogene Daten definiert als „personenbezogene Daten über rassische oder ethnische Herkunft, religiöse Überzeugung, politische Überzeugung, Gewerkschaftszugehörigkeit oder Zugehörigkeit zu einer religiösen, weltanschaulichen oder politischen Organisation, Daten über die Gesundheit oder das Sexualleben, genetische oder biometrische Daten, wenn sie mit einer natürlichen Person verbunden sind.“ Wie aus der nationalen Rechtsprechung hervorgeht, sollte das Sexualleben so ausgelegt werden, dass es auch die sexuelle Orientierung oder Vorlieben der Person umfasst. Insbesondere hat das Oberste Bundesgericht in seiner Rechtsprechung zu gleichgeschlechtlichen Ehen entschieden, dass Diskriminierung aufgrund des „Geschlechts“ auch die „sexuellen Vorlieben“ umfasst⁸⁹ und dass die Freiheit, die „sexuelle Orientierung“ auszuüben, eine „Voraussetzung für die Entfaltung der Persönlichkeit“ ist, die verfassungsrechtlich geschützt ist⁹⁰. Daher entsprechen die Kategorien von Daten, die

⁸⁶ ANPD, Leitfaden zum berechtigten Interesse, S. 16, zur Auslegung des Artikels 10 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁸⁷ ANPD, Leitfaden zum berechtigten Interesse, S. 16.

⁸⁸ ANPD, Leitfaden zum berechtigten Interesse, S. 17.

⁸⁹ Siehe Urteil des Obersten Bundesgerichts Brasiliens, mit dem gleichgeschlechtliche Ehen zugelassen werden und Artikel 3 Abschnitt IV der Bundesverfassung ausgelegt wird, der jede Diskriminierung aufgrund des Geschlechts, der Rasse und der Hautfarbe verbietet. Oberstes Bundesgericht, Entscheidung in der Rechtssache ADI 4277 vom 5. Mai 2011, Nummern 2 und 6. Abrufbar unter: <https://portal.stf.jus.br/peticaoInicial/verPeticaoInicial.asp?base=ADI&numProcesso=4277>.

⁹⁰ Siehe Urteil des Obersten Bundesgerichts Brasiliens, mit dem gleichgeschlechtliche Ehen zugelassen werden, S. 14: „Als unabdingbare Voraussetzung für die Entwicklung der menschlichen Persönlichkeit – des höchsten durch die Bundesverfassung geschützten Wertes – ist es unerlässlich, alle rechtlichen Hindernisse zu beseitigen, die eine – auch nur potenzielle – Einschränkung der uneingeschränkten Ausübung der Freiheit darstellen, die jeder Mensch bei der uneingeschränkten Ausübung seiner sexuellen Orientierung hat“ (Hervorhebung hinzugefügt).

nach brasilianischem Recht als sensible Daten gelten, denen nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679.

- (55) Die brasilianischen Gerichte haben die Definition sensibler personenbezogener Daten im Rahmen des LGPD auf andere Arten von Informationen ausgeweitet, die zur Diskriminierung natürlicher Personen verwendet werden könnten⁹¹. Diese Auslegung ergibt sich aus dem Recht auf Schutz vor Diskriminierung nach brasilianischem Recht, wie es auch in Artikel 6 Ziffer IX LGPD zum Ausdruck kommt. Insbesondere wurde in der brasilianischen Rechtsprechung klargestellt, dass Informationen über Strafregister als sensible Daten zu betrachten sind⁹².
- (56) Die Verarbeitung sensibler Daten nach dem LGPD ist nur zulässig, wenn die betroffene Person oder ihr gesetzlicher Vertreter ihre „spezifische und eindeutige“ Einwilligung für bestimmte Zwecke erteilt hat⁹³. Es gelten die in den Erwägungsgründen 46 bis 48 dieses Beschlusses beschriebenen Bedingungen für eine gültige Einwilligung.
- (57) Nach Artikel 11 Ziffer II LGPD kann die Verarbeitung sensibler Daten ohne ausdrückliche Einwilligung der betroffenen Person unter den folgenden Voraussetzungen erfolgen: 1) wenn die Verarbeitung für die Erfüllung einer rechtlichen oder regulatorischen Verpflichtung des für die Verarbeitung Verantwortlichen erforderlich ist (Buchstabe a), 2) wenn dies für die Verarbeitung durch die öffentliche Verwaltung zur Durchführung der in Gesetzen oder sonstigen Vorschriften vorgesehenen öffentlichen Maßnahmen erforderlich ist (Buchstabe b), 3) zum Schutz des Lebens oder der körperlichen Unversehrtheit der betroffenen Person oder eines Dritten (Buchstabe e), 4) zur Ausübung von Rechten, auch in vertraglichen und gerichtlichen Verwaltungs- und Schiedsverfahren, nach brasilianischem Recht (Buchstabe d), 5) zum Schutz der Gesundheit der betroffenen Person, ausschließlich in Verfahren, die von Angehörigen der Gesundheitsberufe, Gesundheitsdiensten oder Gesundheitsbehörden durchgeführt werden (Buchstabe f), 6) durch Forschungseinrichtungen zur Durchführung von Studien, wobei sicherzustellen ist, dass die Daten nach Möglichkeit anonymisiert werden (Buchstabe c) und 7) zur Verhinderung von Betrug und zur Gewährleistung der Sicherheit der betroffenen Personen bei Identifizierungs- und Authentifizierungsverfahren durch Registrierung in elektronischen Systemen. Folglich sind die Gründe für die Verarbeitung sensibler Daten im Rahmen des LGPD und der Verordnung (EU) 2016/679 ähnlich.

2.4.5. Zweckbindung

- (58) Personenbezogene Daten sollten für einen bestimmten Zweck und in einer Weise erhoben werden, die mit dem Zweck der Verarbeitung nicht unvereinbar ist.
- (59) Artikel 6 Ziffer I LGPD sieht vor, dass personenbezogene Daten für einen „berechtigten, spezifischen und eindeutigen Zweck, über den die betroffene Person unterrichtet wird“, verarbeitet werden sollten, ohne dass eine Weiterverarbeitung möglich ist, die mit dem ursprünglichen Zweck „unvereinbar“ ist. Dieser Grundsatz und sein Wortlaut sind nahezu identisch mit dem entsprechenden Grundsatz in

⁹¹ Oberstes Arbeitsgericht, Entscheidung in der Rechtssache TST-E-RR-933-49.2012.5.10.0001, Dezember 2021. Abrufbar unter: <https://www.jusbrasil.com.br/jurisprudencia/tst/713123452/inteiro-teor-713123472>.

⁹² Oberstes Arbeitsgericht, Entscheidung in der Rechtssache TST-E-RR-933-49.2012.5.10.0001, Dezember 2021.

⁹³ Artikel 11 Ziffer I des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

Artikel 5 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679. In Artikel 6 Ziffer II LGPD ist ferner festgelegt, dass jede Verarbeitung mit den der betroffenen Person mitgeteilten Zwecken vereinbar sein muss.

- (60) Aus den Leitlinien der ANPD geht hervor, dass der Verantwortliche, um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbar ist, eine Verbindung zwischen den beiden Verarbeitungszwecken nachweisen und die „berechtigten Erwartungen“ der betroffenen Personen berücksichtigen muss⁹⁴. Im Falle einer Verarbeitung für weitere kompatible Zwecke gelten die Grundsätze und Pflichten des LGPD, insbesondere um sicherzustellen, dass der neue Zweck spezifisch ist, und um den Schutz der Rechte der betroffenen Personen zu gewährleisten. Dies gilt auch für die Weiterverarbeitung von Daten, die von der betroffenen Person „offensichtlich zugänglich gemacht“ wurden oder öffentlich zugänglich sind⁹⁵.

2.4.6. Richtigkeit der Daten und Datenminimierung

- (61) Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Ferner müssen sie dem Zweck angemessen und dafür maßgeblich sein und dürfen das für die Zwecke der Verarbeitung notwendige Maß nicht überschreiten.
- (62) Diese Grundsätze werden durch die Grundsätze „Qualität der Daten“ und „Notwendigkeit“ in Artikel 6 Ziffern III und V LGPD gewährleistet. Gemäß Artikel 6 Ziffer V LGPD müssen der Verantwortliche und der Auftragsverarbeiter sicherstellen, dass die personenbezogenen Daten im Hinblick auf die Zwecke, zu denen diese Daten verarbeitet werden, richtig, eindeutig, maßgeblich und aktuell sind. Artikel 6 Ziffer III LGPD legt die „Beschränkung der Verarbeitung auf das erforderliche Mindestmaß“, das zum Erreichen eines bestimmten Zwecks bzw. bestimmter Zwecke erforderlich ist, fest, „um Daten zu erfassen, die in Bezug auf diese(n) Zweck(e) maßgeblich, verhältnismäßig und nicht übermäßig sind“. Diese Grundsätze ähneln denen in Artikel 5 Absatz 1 Buchstaben c und d der Verordnung (EU) 2016/679.

2.4.7. Begrenzung der Speicherdauer

- (63) Daten dürfen grundsätzlich nur so lange gespeichert werden, wie dies für die Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, erforderlich ist.
- (64) Die in Artikel 6 Ziffern I, III und IV LGPD niedergelegten Grundsätze „Zweck“, „Notwendigkeit“ und „Zugang“ enthalten Anforderungen an die Begrenzung der Speicherdauer. Damit wird die Möglichkeit, Daten zu speichern, auf das im Zusammenhang mit einem „berechtigten, spezifischen und eindeutigen“ Zweck erforderliche Mindestmaß begrenzt, und es wird vorgeschrieben, dass die betroffenen Personen über die Dauer der Speicherung informiert werden müssen.
- (65) Darüber hinaus ist Kapitel II Abschnitt IV LGPD der „Beendigung der Datenverarbeitung“ gewidmet. Gemäß diesem Abschnitt müssen nach Artikel 16 LGPD alle personenbezogenen Daten nach Beendigung der Verarbeitung für einen

⁹⁴ ANPD, Leitfaden zum berechtigten Interesse, S. 26 und Anhang 2.

⁹⁵ Artikel 7 Absatz 7 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz. Siehe auch Erwägungsgrund 48 dieses Beschlusses. Das Konzept der „offensichtlich zugänglichen“ Daten findet sich auch in der Verordnung (EU) 2016/679, während sich „öffentlich zugängliche“ Daten auf Informationen beziehen, die nach dem brasilianischem Gesetz Nr. 12.527 vom 18. November 2011 über den Zugang zu Informationen in öffentlichen Registern oder Datenbanken verfügbar sind. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm.

bestimmten Zweck gelöscht werden. Diese Anforderungen in Verbindung mit den im LGPD niedergelegten Grundsätzen „Zweck“, „Notwendigkeit“ und „Zugang“ sind mit den sich aus Artikel 5 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 ergebenden Verpflichtungen vergleichbar.

- (66) Nach den in Artikel 16 LGPD festgelegten strengen Ausnahmen dürfen Daten in folgenden Fällen weiterhin aufbewahrt und gespeichert werden: 1) zur Einhaltung rechtlicher und regulatorischer Verpflichtungen, 2) zu Forschungszwecken, wobei nach Möglichkeit die Anonymisierung der Daten zu gewährleisten ist, 3) bei Übermittlung an Dritte gemäß den Anforderungen des LGPD oder 4) bei ausschließlicher Verwendung durch den Verantwortlichen, sofern die Daten anonymisiert sind und der Zugang Dritter zu diesen Daten untersagt ist.
- (67) Die im LGPD festgelegte und in den Erwägungsgründen 68 bis 78 dieses Beschlusses beschriebene Anforderung an die Datensicherheit gilt für gespeicherte Daten.

2.4.8. Datensicherheit

- (68) Personenbezogene Daten müssen in einer Weise verarbeitet werden, die ihre Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Zu diesem Zweck müssen Betreiber geeignete technische oder organisatorische Maßnahmen treffen, um personenbezogene Daten vor möglichen Bedrohungen zu schützen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik und der damit verbundenen Kosten bewertet werden.
- (69) Dieser Grundsatz wird durch Artikel 6 Ziffer VII LGPD gewährleistet, der den Einsatz „technischer und administrativer Maßnahmen“ zum Schutz personenbezogener Daten vor „unbefugtem Zugriff und unbeabsichtigter oder unrechtmäßiger“ Verarbeitung, einschließlich „der Vernichtung, des Verlusts, der Veränderung, der Weitergabe oder der Verbreitung“ von Daten, vorschreibt. Um diese Sicherheitsrisiken zu verringern, schreibt Artikel 6 Ziffer VIII LGPD vor, Maßnahmen zur „Verhinderung von Schäden aufgrund der Verarbeitung personenbezogener Daten“ zu treffen.
- (70) Nach Artikel 44 LGPD ist die Verarbeitung personenbezogener Daten unrechtmäßig, wenn sie nicht den Sicherheitsstandards entspricht, die eine betroffene Person berechtigterweise erwarten darf. Das angemessene Sicherheitsniveau muss unter anderem unter Berücksichtigung des Folgenden festgelegt werden: 1) der besonderen Umstände, unter denen die Verarbeitung erfolgt, 2) des zu erwartenden vertretbaren Risikos und 3) der zum Zeitpunkt der Durchführung verfügbaren Verarbeitungstechniken⁹⁶.
- (71) Zur Umsetzung des Grundsatzes der Datensicherheit legt das LGPD in Kapitel VII Abschnitt I „Sicherheit und Geheimhaltung von Daten“ eine Reihe von Anforderungen fest. Nach diesem Abschnitt sind der Verantwortliche und der Auftragsverarbeiter nach Artikel 46 LGPD verpflichtet, „sichere, technische und administrative Maßnahmen zu treffen, um personenbezogene Daten vor unbefugtem Zugriff sowie vor unbeabsichtigter oder unrechtmäßiger Verarbeitung zu schützen“, wie z. B. „Vernichtung, Verlust, Veränderung, Weitergabe oder jede Art von unzulässiger oder unrechtmäßiger Verarbeitung“. Diese Maßnahmen sind „von der Konzeptionsphase

⁹⁶ Artikel 44 Ziffern I bis III des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

des Produkts oder der Dienstleistung bis zu seiner Ausführung“ einzuhalten⁹⁷. Artikel 47 LGPD verpflichtet alle an der Verarbeitung beteiligten Parteien allgemein, die Sicherheitsanforderungen einzuhalten. Diese Verpflichtungen ähneln denen, die in Artikel 32 der Verordnung (EU) 2016/679 festgelegt sind.

- (72) In Artikel 44 LGPD ist ferner festgelegt, dass ein Verantwortlicher oder ein Auftragsverarbeiter, der es versäumt, Sicherheitsmaßnahmen zu treffen, für Schäden haftbar gemacht werden kann, die im Falle einer Verletzung der Sicherheit entstehen⁹⁸. Die ANPD kann auch technische Mindestsicherheitsstandards festlegen, um die Einhaltung der Verpflichtungen im Bereich der Datensicherheit zu gewährleisten⁹⁹.
- (73) Nach Artikel 48 LGPD ist der Verantwortliche im Falle eines Sicherheitsvorfalls, der ein Risiko für die betroffenen Personen darstellen oder ihnen erhebliche Schäden zufügen kann, verpflichtet, sowohl die ANPD als auch die betroffenen Personen zu benachrichtigen. Diese Benachrichtigung muss innerhalb einer von der ANPD festgelegten angemessenen Frist erfolgen und mindestens Folgendes umfassen: 1) eine Beschreibung der Art der betroffenen personenbezogenen Daten, 2) Angaben zur Identifizierung der betroffenen Personen, 3) Angabe der technischen und sicherheitstechnischen Maßnahmen, die zum Schutz der Daten, unter Wahrung des Geschäfts- und Betriebsgeheimnisses, getroffen wurden, 4) eine Bewertung der mit dem Vorfall verbundenen Risiken, 5) eine Erklärung für etwaige Verzögerungen bei der Benachrichtigung und 6) eine Beschreibung der Maßnahmen, die zur Minderung oder Behebung des entstandenen Schadens ergriffen wurden oder werden sollen. Der im LGPD verfolgte Ansatz ähnelt weitgehend dem in den Artikeln 33 und 34 der Verordnung (EU) 2016/679 festgelegten Ansatz.
- (74) Die ANPD hat zusätzliche Vorschriften zu Sicherheitsvorfällen im Zusammenhang mit Daten angenommen, um beispielsweise die Definition eines „Vorfalls“ und die Frist für die Meldung eines Vorfalls zu präzisieren¹⁰⁰.
- (75) In Artikel 3 Ziffer XII der Verordnung über die Meldung von Sicherheitsvorfällen wird ein Sicherheitsvorfall definiert als „jedes bestätigte unerwünschte Ereignis im Zusammenhang mit der Verletzung der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Sicherheit personenbezogener Daten“. Nach Artikel 48 LGPD müssen Datenschutzverletzungen und Sicherheitsvorfälle, die Risiken für die betroffenen Personen mit sich bringen können, stets der Datenschutzbehörde (ANPD) und den betroffenen Personen mitgeteilt werden. In Artikel 5 der Verordnung über die Meldung von Sicherheitsvorfällen wird klargestellt, dass ein Sicherheitsvorfall ein Risiko für betroffene Personen mit sich bringen kann, wenn er deren Interessen und Grundrechte beeinträchtigen kann und wenn er mindestens eine der folgenden Arten von Daten betrifft: 1) sensible personenbezogene Daten, 2) Daten von Kindern, Jugendlichen oder älteren Menschen, 3) Finanzdaten, 4) Authentifizierungsdaten in Systemen, 5) Daten, die dem Rechts-, Justiz- oder Berufsgeheimnis unterliegen oder 6) Großdatenbanken. Darüber hinaus wird davon ausgegangen, dass ein Sicherheitsvorfall die grundlegenden Interessen und Rechte der betroffenen Personen

⁹⁷ Artikel 46 Absatz 2 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁹⁸ Artikel 44, Hauptabsatz des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

⁹⁹ Artikel 46 Absatz 1 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹⁰⁰ ANPD, Verordnung über die Meldung von Sicherheitsvorfällen, April 2024. Abrufbar unter: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>.

erheblich beeinträchtigt, wenn 1) er der Ausübung von Rechten oder der Nutzung einer Dienstleistung entgegenstehen kann oder 2) den betroffenen Personen materielle oder immaterielle Schäden wie beispielsweise Diskriminierung, Verletzung der körperlichen Unversehrtheit, des Rechts am eigenen Bild und des guten Rufs, Finanzbetrug oder Identitätsdiebstahl entstehen können¹⁰¹.

- (76) Die Meldung eines Sicherheitsvorfalls an die ANPD und die betroffenen Personen muss innerhalb von drei Werktagen, nachdem der Verantwortliche davon Kenntnis erlangt hat, erfolgen¹⁰². In der verbindlichen Verordnung über die Meldung von Sicherheitsvorfällen wird für die Verantwortlichen klargestellt, welche Informationen der ANPD und den betroffenen Personen zu übermitteln sind. Die Meldung an die betroffenen Personen muss insbesondere Folgendes umfassen: 1) eine Beschreibung der Art und der Kategorie der betroffenen personenbezogenen Daten, 2) die zum Schutz der Daten getroffenen technischen und sicherheitstechnischen Maßnahmen, 3) die mit dem Sicherheitsvorfall verbundenen Risiken unter Angabe der möglichen Auswirkungen auf die betroffenen Personen, 4) die Gründe für die Verzögerung, falls die Meldung nicht innerhalb von 72 Stunden erfolgte, 5) die Maßnahmen, die gegebenenfalls ergriffen wurden oder werden, um die Auswirkungen des Sicherheitsvorfalls rückgängig zu machen oder abzumildern, 6) das Datum, an dem der Sicherheitsvorfall entdeckt wurde, und 7) die Kontaktdaten für Informationen und gegebenenfalls die Kontaktdaten der zuständigen Person¹⁰³. Bei der Meldung des Vorfalls an die betroffenen Personen haben die Verantwortlichen eine „einfache und leicht verständliche Sprache“ zu verwenden¹⁰⁴. Die Meldung muss unmittelbar und individuell erfolgen, wenn es möglich ist, die betroffenen Personen zu identifizieren¹⁰⁵.
- (77) Darüber hinaus kann die ANPD, wenn dies zum Schutz der Rechte der betroffenen Personen erforderlich ist, die Schwere des Vorfalls bewerten und den Verantwortlichen anweisen, bestimmte Maßnahmen zu ergreifen¹⁰⁶. Dies kann die Offenlegung des Sicherheitsvorfalls über geeignete Medienkanäle sowie die Durchführung von Abhilfemaßnahmen oder mildernden Maßnahmen umfassen. Der Verantwortliche muss ein Register der Datensicherheitsvorfälle führen¹⁰⁷.
- (78) Schließlich verknüpft das LGPD seine Standards für „bewährte Verfahren und (Daten-)Governance“ mit den Anforderungen an die Datensicherheit, um unter anderem Risiken bei der Datenverarbeitung zu mindern¹⁰⁸. Dazu gehört auch die Förderung der Annahme interner Datenschutz-Governance-Programme zur Bewertung und Minderung von Risiken¹⁰⁹.

2.4.9. Transparenz

¹⁰¹ Artikel 5 Absatz 1, ANPD, Verordnung über die Meldung von Sicherheitsvorfällen, April 2024.

¹⁰² Artikel 6 und 9, ANPD, Verordnung über die Meldung von Sicherheitsvorfällen, April 2024.

¹⁰³ Artikel 9 Ziffern I bis VII, ANPD, Verordnung über die Meldung von Sicherheitsvorfällen, April 2024.

¹⁰⁴ Artikel 9 Absatz 1 Ziffer I, ANPD, Verordnung über die Meldung von Sicherheitsvorfällen, April 2024.

¹⁰⁵ Artikel 9 Absatz 1 Ziffer II, ANPD, Verordnung über die Meldung von Sicherheitsvorfällen, April 2024.

¹⁰⁶ Artikel 48 Absatz 2 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹⁰⁷ Artikel 10, ANPD, Verordnung über die Meldung von Sicherheitsvorfällen, April 2024.

¹⁰⁸ Artikel 49 und 50 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹⁰⁹ Artikel 50, Hauptsatz und Absatz 1 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

- (79) Betroffene Personen müssen über die Hauptmerkmale der Verarbeitung ihrer personenbezogenen Daten unterrichtet werden.
- (80) Nach einem Ansatz, der mit Artikel 12 der Verordnung (EU) 2016/679 vergleichbar ist, ist in Artikel 6 Ziffer VI LGPD festgelegt, dass die betroffenen Personen klare, präzise und leicht zugängliche Informationen sowohl über die Durchführung der Datenverarbeitung als auch über die jeweiligen Verarbeitungsbeauftragten erhalten, wobei das „Geschäfts- und Betriebsgeheimnis“ zu wahren ist.
- (81) Artikel 9 LGPD enthält eine Liste der Informationen, die den betroffenen Personen über die Verarbeitung von Daten zur Verfügung zu stellen sind und die Folgendes umfassen: 1) den bestimmten Zweck der Verarbeitung, 2) Art und Dauer der Verarbeitung, 3) Angaben zu dem Verantwortlichen, 4) die Kontaktdaten des Verantwortlichen, 5) Informationen über die Verarbeitung der Daten durch den Verantwortlichen und den Zweck, 6) die Zuständigkeiten der mit der Verarbeitung beauftragten Stellen und 7) die Rechte der betroffenen Personen, einschließlich Informationen über die Ausübung dieser Rechte.
- (82) Die Beschränkung in Bezug auf das „Geschäfts- und Betriebsgeheimnis“ gemäß Artikel 6 Ziffer VI sowie andere Bestimmungen des LGPD sollten im Lichte des brasilianischen Gesetzes über den Zugang zu Informationen¹¹⁰ ausgelegt werden. Das Gesetz über den Zugang zu Informationen legt in der Regel die Offenlegung von Informationen fest, die in Registern oder Dokumenten öffentlicher Stellen enthalten sind¹¹¹. Ausnahmen – d. h. Beschränkungen des Zugangs zu Dokumenten und Informationen – müssen begründet und gesetzlich vorgesehen sein¹¹². Das Geschäfts- und Betriebsgeheimnis ist eine dieser Ausnahmen, für die es eine spezifische Rechtsvorschrift gibt, die den Schutz von „Informationen über die Geschäftstätigkeit natürlicher oder juristischer Personen des Privatrechts, die von anderen Stellen oder Einrichtungen in Ausübung ihrer Tätigkeit der Kontrolle, Regulierung und Überwachung einer wirtschaftlichen Tätigkeit erlangt werden und deren Offenlegung einen Wettbewerbsvorteil für andere Wirtschaftsteilnehmer darstellen könnte“, gewährleisten soll¹¹³. Die Bestimmungen des LGPD, die sich auf das „Geschäfts- und Betriebsgeheimnis“ beziehen, sind daher so auszulegen, dass die Verarbeitung und anderweitige Offenlegung von Informationen weder Geschäftsgeheimnisse offenlegen noch Wettbewerbsvorteile für andere Wirtschaftsteilnehmer schaffen darf, wobei die Ziele des Schutzes personenbezogener Daten zu erfüllen sind. Dies bedeutet, dass im Hinblick auf den Grundsatz der Transparenz und im gesamten Text des LGPD die Einschränkung des „Geschäfts- und Betriebsgeheimnisses“ nicht als pauschaler Versagungsgrund für die Einhaltung der Rechtsvorschriften zu verstehen ist, sondern vielmehr, dass spezifische Vorkehrungen getroffen werden müssen, um die Offenlegung von Informationen in einer Weise sicherzustellen, die diese Interessen schützt.

2.4.10. Rechte des Einzelnen

- (83) Betroffene Personen sollten über bestimmte Rechte verfügen, die gegenüber dem Verantwortlichen geltend gemacht werden können, insbesondere das Recht auf

¹¹⁰ Gesetz Nr. 12.527 vom 18. November 2011 über den Zugang zu Informationen. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

¹¹¹ Artikel 6 und 9 des Gesetzes Nr. 12.527 vom 18. November 2011 über den Zugang zu Informationen.

¹¹² Artikel 22 des Gesetzes Nr. 12.527 vom 18. November 2011 über den Zugang zu Informationen.

¹¹³ Artikel 5 Absatz 2 des Erlasses Nr. 7.721 vom 16. Mai 2012 im Zusammenhang mit dem Gesetz Nr. 12.527 vom 18. November 2011 über den Zugang zu Informationen.

Auskunft über die Daten, das Recht auf Berichtigung, das Recht auf Löschung der Daten, das Recht auf Widerspruch gegen die Verarbeitung, das Recht auf Datenübertragbarkeit und die Rechte im Zusammenhang mit der automatisierten Verarbeitung von Daten. Diese Rechte können Beschränkungen unterliegen, sofern diese Beschränkungen notwendig und verhältnismäßig sind, um bestimmte Ziele von allgemeinem öffentlichem Interesse zu schützen.

- (84) In Kapitel III LGPD werden die Rechte der betroffenen Person in ähnlicher Weise festgelegt wie in den Artikeln 15 bis 22 der Verordnung (EU) 2016/679. Die Ausübung aller Rechte muss kostenlos sein, und die betroffenen Personen müssen über ihre Rechte informiert werden¹¹⁴. Nach Artikel 21 LGPD dürfen Daten, die die Ausübung von Rechten durch eine betroffene Person betreffen, nicht zu ihrem Nachteil verwendet werden. Betroffene Personen können zur Wahrung ihrer Interessen und Rechte einzeln oder kollektiv vor Gericht Rechtsmittel einlegen¹¹⁵.
- (85) Die für die Verarbeitung Verantwortlichen müssen die Auftragsverarbeiter, an die die Daten möglicherweise weitergegeben wurden, „unmittelbar“ über die Anträge betroffener Personen auf Berichtigung, Löschung, Anonymisierung, Einschränkung und Widerspruch in Kenntnis setzen, um sicherzustellen, dass diesen Anträgen von allen Beteiligten entsprochen werden kann¹¹⁶.
- (86) Nach Artikel 9 und Artikel 18 Ziffer II LGPD haben betroffene Personen ein Recht auf Information und Zugang, um „jederzeit“ Informationen über die Verarbeitung ihrer Daten zu erhalten¹¹⁷. Dies umfasst 1) die Identität des Verantwortlichen (Ziffer III), 2) die Kontaktdaten des Verantwortlichen (Ziffer IV), 3) Informationen über den spezifischen Zweck der Verarbeitung (Ziffer I), 4) Informationen über die mögliche Weitergabe von Daten (Ziffer V), 5) Art und Dauer der Verarbeitung (Ziffer II), 6) das Bestehen von Rechten betroffener Personen, einschließlich des Rechts, bei der Datenschutzbehörde Beschwerde einzulegen, und 7) die Zuständigkeiten der Auftragsverarbeiter. Darüber hinaus verpflichtet Artikel 10 Absatz 2 LGPD den Verantwortlichen zu Transparenz hinsichtlich der Verarbeitung auf der Grundlage eines berechtigten Interesses. Ebenso ist in Artikel 9 der Datenübermittlungsverordnung festgelegt, dass betroffene Personen im Falle der Übermittlung personenbezogener Daten zu unterrichten sind.
- (87) In Artikel 19 LGPD wird die Art und Weise, wie betroffenen Personen Zugang zu ihren personenbezogenen Daten zu gewähren ist, näher ausgeführt. Auf Antrag einer betroffenen Person ist der Zugang zu personenbezogenen Daten wie folgt zu gewähren: unverzüglich „in einem vereinfachten Format“ oder innerhalb von 15 Tagen durch eine klare und vollständige Erklärung¹¹⁸. Ferner ist in Artikel 19 Absatz 1 LGPD festgelegt, dass die Verantwortlichen personenbezogene Daten in einem Format speichern müssen, das die Ausübung des Rechts auf Zugang erleichtert.

¹¹⁴ Artikel 18 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹¹⁵ Artikel 22 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹¹⁶ Artikel 18 Absatz 6 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹¹⁷ Artikel 6 Ziffer VI, Artikel 18 und Artikel 19 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹¹⁸ Artikel 19 Ziffern I und II des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

Die betroffene Person kann entscheiden, ob sie ihre Informationen in elektronischer Form oder auf Papier erhalten möchte¹¹⁹.

- (88) Die betroffenen Personen haben nach Artikel 18 Ziffer III LGPD das Recht, die Berichtigung unvollständiger, unrichtiger oder veralteter Daten zu verlangen (Recht auf Berichtigung).
- (89) Nach Artikel 18 Ziffern IV und VI LGPD können natürliche Personen die Löschung ihrer Daten verlangen, wenn 1) es sich um unnötige oder übermäßige Daten handelt, 2) es sich um Daten handelt, die mit Einwilligung der betroffenen Person verarbeitet wurden, oder 3) die Daten unrechtmäßig verarbeitet werden. Darüber hinaus ist in Kapitel II Abschnitt IV LGPD in Bezug auf die „Beendigung der Datenverarbeitung“ festgelegt, dass die Verarbeitung von Daten einzustellen ist, wenn eine betroffene Person entweder Widerspruch gegen die Verarbeitung einlegt oder ihre Einwilligung zur Verarbeitung widerruft¹²⁰. Anschließend müssen die Daten nach Beendigung der Verarbeitung gelöscht werden¹²¹. Diese Bestimmungen erweitern in ihrer Gesamtheit somit indirekt den Anwendungsbereich des Rechts auf Löschung nach dem LGPD.
- (90) Natürliche Personen haben das Recht, im Falle der Nichteinhaltung des LGPD der Verarbeitung von Daten auf einer anderen Rechtsgrundlage als der Einwilligung zu widersprechen (Widerspruchsrecht)¹²². Darüber hinaus haben betroffene Personen gemäß Artikel 15 und Artikel 18 Ziffer IV LGPD das Recht, die Verarbeitung von Daten zu beschränken („Sperrung“). Dieses Recht kann insbesondere dann geltend gemacht werden, wenn die verarbeiteten Daten unnötig oder übermäßig sind oder wenn die Daten in einer Weise verarbeitet werden, die nicht mit dem LGPD vereinbar ist¹²³. Nach Artikel 15 Ziffer II LGPD dürfen Daten auf der Grundlage einer „Mitteilung“ der betroffenen Person an den Verantwortlichen nicht mehr verarbeitet werden. Obgleich diese Bestimmung dem „öffentlichen Interesse“ unterliegt, das weit ausgelegt wird, sieht sie einen weiten Anwendungsbereich für ein indirektes Widerspruchsrecht in einer Weise vor, die dem in der Verordnung (EU) 2016/679 vorgesehenen Widerspruchsrecht entspricht.
- (91) Natürliche Personen haben das Recht, eine „vollständige elektronische Kopie“ ihrer Daten zu verlangen, um die Nutzung durch andere Stellen zu ermöglichen (Recht auf Übertragbarkeit)¹²⁴. Ähnlich wie in der EU können betroffene Personen diese Kopie nur dann anfordern, wenn die Daten auf der Grundlage einer Einwilligung oder eines Vertrags verarbeitet wurden.
- (92) Auch wenn jede Entscheidung, die auf einer automatisierten Verarbeitung von in der EU erhobenen Daten beruht, in der Regel von einem Verantwortlichen getroffen wird

¹¹⁹ Artikel 19 Absatz 2 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹²⁰ Siehe Artikel 15 Ziffer III des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), in dem sich die „Mitteilung der betroffenen Person“ unter anderem auf einen Widerruf der Einwilligung bezieht (wie im Artikel angegeben). Die Bedeutung von „Mitteilung“ ist nicht auf dieses Szenario beschränkt und ermöglicht es betroffenen Personen, die Einstellung der Verarbeitung zu verlangen.

¹²¹ Artikel 16 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹²² Artikel 18 Absatz 2 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹²³ Artikel 18 Ziffer IV des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹²⁴ Artikel 19 Absatz 3 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

(der in einer direkten Beziehung zu der betroffenen Person steht und somit unmittelbar in den Anwendungsbereich der Verordnung (EU) 2016/679 fällt), ist anzumerken, dass das LGPD diese Art der Verarbeitung in ähnlicher Art und Weise regelt wie Artikel 22 der Verordnung (EU) 2016/679. Erstens wird in Artikel 6 Ziffer IX LGPD der Grundsatz der Nichtdiskriminierung als Datenschutzgrundsatz anerkannt, wonach es verboten ist, Daten zu unrechtmäßigen oder missbräuchlichen diskriminierenden Zwecken zu verarbeiten. Dieser Grundsatz gilt für jede Verarbeitung und ist im Zusammenhang mit der automatisierten Verarbeitung besonders relevant. Nach Artikel 20 LGPD haben die betroffenen Personen das Recht, „die Überprüfung von Entscheidungen zu verlangen, die ausschließlich auf der Grundlage einer automatisierten Verarbeitung von Daten getroffen wurden, die ihre Interessen berühren, einschließlich Entscheidungen, die dazu dienen, ihr persönliches, berufliches, Verbraucher- und Kreditprofil oder Aspekte ihrer Persönlichkeit zu bestimmen“. Bei der Beantwortung eines Antrags einer betroffenen Person muss der Verantwortliche klare Informationen über „die Kriterien und das Verfahren für die auf der Grundlage einer automatisierten Verarbeitung getroffenen Entscheidung“ bereitstellen¹²⁵. Für den Fall, dass diese Informationen der betroffenen Person aus Gründen des „Geschäfts- und Betriebsgeheimnisses“ nicht zur Verfügung gestellt werden können, ist die ANPD befugt, eine Prüfung durchzuführen, um diskriminierende Aspekte der automatisierten Verarbeitung personenbezogener Daten zu überprüfen¹²⁶. Folglich kann das „Geschäfts- und Betriebsgeheimnis“ nicht als Grund dafür herangezogen werden, den Antrag der betroffenen Person abzulehnen.

- (93) Artikel 23 LGPD bestimmt, dass für das Verfahren und die Frist für die Ausübung der Rechte betroffener Personen bei der Verarbeitung durch Behörden besondere Rechtsvorschriften gelten¹²⁷. So regelt beispielsweise das brasilianische *Habeas-Data*-Gesetz das Recht natürlicher Personen auf Zugang zu Informationen über Daten, die in Registern oder Datenbanken der Regierung oder einer öffentlichen Einrichtung gespeichert sind¹²⁸. Das brasilianische *Habeas-Data*-Gesetz enthält besondere Bestimmungen zum Recht auf Zugang, das innerhalb von zehn Tagen nach dem Antrag einer natürlichen Person gewährt werden muss, und zum Recht auf Berichtigung, das innerhalb von 15 Tagen nach einem Antrag gewährt werden muss¹²⁹. In ähnlicher Weise sieht das brasilianische Bundesverwaltungsverfahrensgesetz ein Recht auf Information und Zugang für natürliche Personen im Rahmen von Verwaltungsverfahren vor¹³⁰. Das brasilianische Gesetz über den Zugang zu Informationen sieht zudem Informations- und Transparenzpflichten für Behörden, öffentliche Unternehmen und die drei Gewalten

¹²⁵ Artikel 20 Absatz 1 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹²⁶ Artikel 20 Absatz 2 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹²⁷ Artikel 23 Absatz 3 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹²⁸ Gesetz Nr. 9.507 vom 12. November 1997, brasilianisches Habeas-Data-Gesetz. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/leis/19507.htm.

¹²⁹ Artikel 7 und 8 des Gesetzes Nr. 9.507 vom 12. November 1997, brasilianisches Habeas-Data-Gesetz. Das Gesetz sieht Rechtsbehelfe für den Fall vor, dass dem Antrag der natürlichen Person nicht nachgekommen wird.

¹³⁰ Siehe insbesondere Artikel 6 des Gesetzes Nr. 9.784 vom 29. Januar 1999, Bundesverwaltungsverfahrensgesetz. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/leis/19784.htm. Das Gesetz legt Verfahren und Fristen für die Kommunikation mit natürlichen Personen sowie Rechtsbehelfe bei Verstößen fest.

(Legislative, Exekutive und Judikative) in Brasilien vor¹³¹. Die Bestimmungen dieser Gesetze stärken das Recht auf Zugang zu Informationen, das nach dem LGPD für die Verarbeitung von Daten durch Behörden festgelegt ist. Wenn diese Rechtsvorschriften keine besonderen Rechte im Rahmen des LGPD vorsehen (z. B. Rechte im Zusammenhang mit der automatisierten Entscheidungsfindung), können betroffene Personen diese Rechte im Rahmen des LGPD ausüben.

- (94) Jeder Verstoß gegen die Rechte betroffener Personen wird von der ANPD je nach maßgeblichem Faktor entweder als „mittlere“ oder „schwerwiegende“ Rechtsverletzung behandelt und kann daher mit den höchsten Sanktionen und Geldbußen geahndet werden. Wichtig ist, dass gemäß der Verordnung über Sanktionen der ANPD allein die Tatsache, dass ein Recht einer betroffenen Person durch einen Verstoß beeinträchtigt wurde, bedeutet, dass ein solcher Verstoß nicht als „leicht“ angesehen werden kann¹³².
- (95) Seit Inkrafttreten des LGPD gehen bei der ANPD immer wieder Beschwerden und Anfragen von natürlichen Personen bezüglich ihrer Datenschutzrechte ein¹³³. Diese Zahlen sind seit Juli 2024, nachdem die ANPD eine modernisierte und benutzerfreundliche Plattform für die Einreichung von Anträgen und Beschwerden eingeführt hat, deutlich gestiegen¹³⁴. Seitdem erhält die ANPD monatlich rund 400 Beschwerden und 100 Anträge von natürlichen Personen¹³⁵.

2.4.11. Weiterübermittlung von Daten

- (96) Das Schutzniveau für personenbezogene Daten, die aus der Union an Datenverantwortliche und Auftragsverarbeiter in Brasilien übermittelt werden, darf nicht durch die Weiterübermittlung dieser Daten an Empfänger in einem Drittland beeinträchtigt werden.
- (97) Solche „Weiterübermittlungen“ stellen aus Sicht des brasilianischen Datenverantwortlichen internationale Übermittlungen aus Brasilien dar.
- (98) Kapitel V des LGPD schafft einen Rahmen für die internationale Übermittlung personenbezogener Daten. Die Bestimmungen dieses Kapitels werden durch eine verbindliche Verordnung über internationale Datenübermittlungen (Datenübermittlungsverordnung) ergänzt, die im August 2024 von der ANPD angenommen wurde¹³⁶.
- (99) In der Datenübermittlungsverordnung wird der Begriff „Übermittlung“ definiert als „Verarbeitungsvorgang, durch den ein Verarbeitungsbeauftragter personenbezogene Daten an einen anderen Verarbeitungsbeauftragten übermittelt, weitergibt oder ihm

¹³¹ Artikel 1, 6 und 9 des Gesetzes Nr. 12.527 vom 18. November 2011, Gesetz über den Zugang zu Informationen.

¹³² Artikel 8 Absatz 2, ANPD, Verordnung über die Berechnung und Anwendung von Verwaltungssanktionen, Februar 2023 (im Folgenden „Verordnung über Sanktionen“). Abrufbar unter: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077>.

¹³³ ANPD, Bericht über das vierte Tätigkeitsjahr der ANPD, November 2023, S. 24-25. Abrufbar unter: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/balanco-de-4-anos-anpd-2024.pdf/view>.

¹³⁴ ANPD, Plattform für natürliche Personen. Abrufbar unter: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados.

¹³⁵ ANPD, Bericht über das vierte Tätigkeitsjahr der ANPD, November 2023, S. 25.

¹³⁶ ANPD, Verordnung über internationale Datenübermittlungen, August 2024. In portugiesischer Sprache abrufbar unter: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396> und in englischer Sprache unter: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulation-on-international-transfer-of-personal-data.pdf>.

Zugang zu ihnen gewährt“ und „internationale Datenübermittlung“ als „Übermittlung personenbezogener Daten in ein anderes Land oder an eine internationale Organisation, der das Land angehört“¹³⁷.

- (100) Die im Rahmen des LGPD und der Datenübermittlungsverordnung festgelegten Vorschriften für internationale Übermittlungen gelten für alle Verarbeitungen, die in den Anwendungsbereich des LGPD fallen. In Artikel 7 der Datenübermittlungsverordnung wird ausdrücklich klargestellt, dass die Anwendbarkeit des LGPD auf eine internationale Datenübermittlung nicht von den für die Verarbeitung verwendeten technischen Mitteln, dem geografischen Standort der Daten oder der physischen Anwesenheit des Verantwortlichen oder des Auftragsverarbeiters abhängt¹³⁸. Ausschlaggebend für die Anwendbarkeit ist vielmehr das Bestehen eines inhaltlichen Zusammenhangs zwischen der Datenverarbeitungstätigkeit und Brasilien.
- (101) Ähnlich wie in den Artikeln 44 bis 49 der Verordnung (EU) 2016/679 sind in Artikel 33 LGPD die Umstände festgelegt, unter denen eine internationale Datenübermittlung „ausschließlich“ zulässig ist. Diese Umstände werden in Artikel 9 der Datenübermittlungsverordnung näher erläutert.
- (102) Eine internationale Datenübermittlung kann erfolgen, wenn die folgenden drei kumulativen Voraussetzungen erfüllt sind: Erstens darf eine internationale Datenübermittlung „nur zu berechtigten, spezifischen und eindeutigen Zwecken erfolgen, die der betroffenen Person mitgeteilt werden, sodass keine Weiterverarbeitung möglich ist, die mit diesen Zwecken unvereinbar ist“¹³⁹. Zweitens muss sich die internationale Datenübermittlung auf eine gültige Rechtsgrundlage gemäß Artikel 7 LGPD (oder Artikel 11 im Falle sensibler Daten) stützen¹⁴⁰. Drittens muss ein „gültiger“ Mechanismus für die Datenübermittlung angewandt werden¹⁴¹.
- (103) Artikel 33 LGPD sieht mehrere Mechanismen für die Datenübermittlung vor.
- (104) Erstens kann ein Angemessenheitsbeschluss in Bezug auf ein Drittland oder eine internationale Organisation erlassen werden (Artikel 33 Ziffer I). Bei der Feststellung, ob ein Drittland oder eine internationale Organisation ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, berücksichtigt die ANPD mehrere Kriterien, die im LGPD und in der Datenübermittlungsverordnung¹⁴² festgelegt sind und den entsprechenden Kriterien nach Unionsrecht ähneln. Dazu gehören 1) die im Bestimmungsland oder für die internationale Organisation geltenden allgemeinen und sektorspezifischen Rechtsvorschriften, die sich unmittelbar auf den Schutz personenbezogener Daten auswirken¹⁴³, 2) die Art der Daten¹⁴⁴, 3) die Gewährleistung, dass das Drittland oder die internationale Organisation ein

¹³⁷ Artikel 3 Ziffern III und IV, ANPD, Verordnung über internationale Datenübermittlungen, August 2024 sowie Artikel 5 Ziffer XV des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹³⁸ Artikel 7, ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

¹³⁹ Artikel 9, ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

¹⁴⁰ Artikel 9 Ziffer I, ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

¹⁴¹ Artikel 9 Ziffer II, ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

¹⁴² Artikel 34 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) und Kapitel V, ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

¹⁴³ Artikel 34 Ziffer I des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) und Artikel 11 Ziffer I, ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

¹⁴⁴ Artikel 34 Ziffer II des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) und Artikel 11 Ziffer II, ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

Schutzniveau für personenbezogene Daten bietet und die Rechte der betroffenen Personen im Einklang mit dem LGPD gewährleistet¹⁴⁵, 4) die Einführung geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung der Datensicherheit und zur Minderung der Risiken nachteiliger Auswirkungen auf die Privatsphäre und andere Grundrechte¹⁴⁶, 5) das Vorhandensein gerichtlicher und institutioneller Mechanismen zur Gewährleistung der Datenschutzrechte, insbesondere durch das Vorhandensein einer unabhängigen Aufsichtsbehörde mit angemessenen Befugnissen und Ressourcen zur Überwachung und Durchsetzung der Datenschutzbestimmungen¹⁴⁷, und 6) alle anderen besonderen Umstände, die für den Kontext der internationalen Datenübermittlung von Bedeutung sind¹⁴⁸.

- (105) Zur Bewertung des Schutzniveaus für personenbezogene Daten im Rahmen eines Angemessenheitsbeschlusses bewertet die ANPD auch Folgendes: 1) die Risiken und Vorteile, die sich aus einem bestimmten Angemessenheitsbeschluss ergeben, wobei unter anderem die Gewährleistung der Grundsätze, der Rechte der betroffenen Person und die im LGPD vorgesehene Datenschutzregelung zu berücksichtigen sind, sowie 2) die Auswirkungen des Beschlusses auf den internationalen Datenverkehr, die diplomatischen Beziehungen, den internationalen Handel und die internationale Zusammenarbeit Brasiliens mit anderen Ländern und internationalen Organisationen¹⁴⁹. Für die Bewertung und den Erlass eines Angemessenheitsbeschlusses ist die ANPD zuständig¹⁵⁰. Derzeit arbeitet die ANPD nur an einem Angemessenheitsbeschluss mit der Europäischen Union.
- (106) Zweitens sieht Artikel 33 Ziffer II vor, dass Datenübermittlungen erfolgen können, wenn die Verantwortlichen „Garantien für die Einhaltung der Grundsätze und Rechte der betroffenen Personen und der Datenschutzbestimmungen“ gemäß LGPD gewährleisten. Dies kann durch Folgendes gewährleistet werden: 1) spezifische Vertragsklauseln (Ziffer II Buchstabe a), 2) Standardvertragsklauseln (Ziffer II Buchstabe b), 3) verbindliche unternehmensinterne Vorschriften (Ziffer II Buchstabe c) oder 4) anerkannte Siegel, Zertifizierungen und Verhaltenskodizes (Ziffer II Buchstabe d).
- (107) Die Verantwortlichen können sich auf spezifische Vertragsbestimmungen für die internationale Übermittlung sowie auf Standardvertragsklauseln stützen, die von der ANPD genehmigt wurden¹⁵¹. Im Rahmen der Datenübermittlungsverordnung hat die ANPD eine Reihe von Mustervertragsklauseln angenommen, die alle einschlägigen Datenschutzerfordernisse (d. h. Rechte betroffener Personen, unabhängige Aufsicht und Überwachung, Datensicherheitsmaßnahmen, Garantien für Weiterübermittlungen

¹⁴⁵ Artikel 34 Ziffer III des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) und Artikel 11 Ziffer III, ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

¹⁴⁶ Artikel 34 Ziffer IV des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) und Artikel 11 Ziffer IV, ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

¹⁴⁷ Artikel 11 Absatz 3, ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

¹⁴⁸ Artikel 34 Ziffer VI des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) und Artikel 11 Ziffer VI, ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

¹⁴⁹ Artikel 12, ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

¹⁵⁰ Das Verfahren für den Erlass eines Angemessenheitsbeschlusses wird in Abschnitt III, Verordnung über internationale Datenübermittlungen vom August 2024 beschrieben.

¹⁵¹ Artikel 35 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

usw.) abdecken¹⁵². Diese Klauseln enthalten Bestimmungen, die von den Vertragsparteien nicht geändert werden dürfen¹⁵³. Die Klauseln sind modular gestaltet, sodass sie an verschiedene Szenarien für die Datenübermittlung angepasst werden können (z. B. vom Verantwortlichen zum Auftragsverarbeiter, von Auftragsverarbeiter zu Auftragsverarbeiter)¹⁵⁴.

- (108) In Bezug auf verbindliche unternehmensinterne Datenschutzvorschriften stellt die ANPD in Kapitel VI der Datenübermittlungsverordnung klar, wie dieser Mechanismus genutzt werden kann und welche Anforderungen an seine Gültigkeit zu erfüllen sind. In der ANPD wird insbesondere auf den „verbindlichen Charakter“ des Instruments für alle „Mitglieder der Gruppe oder des Konzerns“, die sich auf dieses Instrument stützen, auf Anforderungen in Bezug auf die Rechte der betroffenen Personen und deren Ausübung, auf die geltenden Vorschriften zur Haftung und Verantwortlichkeit¹⁵⁵ sowie auf alle obligatorischen Informationen, die verbindliche unternehmensinterne Datenschutzvorschriften enthalten müssen, verwiesen¹⁵⁶. Die verbindlichen unternehmensinternen Datenschutzvorschriften unterliegen der vorherigen Genehmigung durch die ANPD nach einem in Kapitel VIII der Datenübermittlungsverordnung festgelegten Verfahren, wonach die Unternehmen verpflichtet sind, der ANPD vollständige Unterlagen vorzulegen, und das ein Überprüfungsverfahren der ANPD umfasst¹⁵⁷. Die Unternehmen sind ferner verpflichtet, der ANPD alle Angelegenheiten mitzuteilen, die sich auf die Einhaltung des LGPD auswirken können, auch wenn Mitglieder der Gruppe ausländischen Verpflichtungen unterliegen¹⁵⁸. Alle genehmigten verbindlichen unternehmensinternen Datenschutzvorschriften werden auf der Webseite der ANPD veröffentlicht, und die Unternehmen sind verpflichtet, über die durchgeführte internationale Übermittlung in transparenter Weise zu informieren¹⁵⁹.
- (109) Die ANPD kann auch Zertifizierungsstellen benennen, die Siegel, Zertifizierungen oder Verhaltenskodizes für Datenübermittlungen entwickeln¹⁶⁰. Die Entscheidungen und Tätigkeiten dieser Zertifizierungsstellen können von der ANPD überprüft werden,

¹⁵² Anhang II, ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

¹⁵³ Anhang II Abschnitt II, ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

¹⁵⁴ Anhang II Klausel 4, ANPD, Verordnung über internationale Datenübermittlungen, August 2024. Verantwortliche und Auftragsverarbeiter können nach dieser Klausel die ihrer Situation entsprechende „Option“ wählen.

¹⁵⁵ Artikel 3 Ziffer VIII, ANPD, Verordnung über internationale Datenübermittlungen, August 2024. Nach der Definition des Begriffs „verantwortliche Einrichtung“ haftet ein „Unternehmen mit Hauptsitz in Brasilien für jeden Verstoß gegen eine verbindliche unternehmensinterne Datenschutzvorschrift, auch wenn dieser auf eine Handlung eines Mitglieds der Unternehmensgruppe mit Hauptsitz in einem anderen Land zurückzuführen ist“, womit ein ähnlicher Ansatz verfolgt wird wie in Artikel 47 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679.

¹⁵⁶ Artikel 27, ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

¹⁵⁷ Artikel 27, 28 und Kapitel VIII, ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

¹⁵⁸ Artikel 25 Ziffer VIII, ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

¹⁵⁹ Artikel 32, ANPD, Verordnung über internationale Datenübermittlungen, August 2024. In diesem Artikel ist ferner festgelegt, dass Unternehmen verpflichtet sind, die verbindlichen unternehmensinternen Datenschutzvorschriften den betroffenen Personen auf Anfrage zur Verfügung zu stellen.

¹⁶⁰ Artikel 35 Absatz 3 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

die Entscheidungen im Falle der Nichteinhaltung des LGPD überprüfen und widerrufen kann¹⁶¹.

- (110) Schließlich enthält das LGPD eine Liste „bestimmter Fälle“, in denen eine internationale Übermittlung durchgeführt werden kann, wenn sie 1) für die internationale rechtliche Zusammenarbeit zwischen öffentlichen Stellen im Einklang mit dem Völkerrecht erforderlich ist, 2) zum Schutz des Lebens oder der körperlichen Unversehrtheit der betroffenen Person oder eines Dritten erforderlich ist, 3) von der ANPD genehmigt wurde, 4) im Zusammenhang mit einer Verpflichtung im Rahmen der internationalen Zusammenarbeit steht, 5) zur Erfüllung einer politischen Maßnahme oder einer rechtlichen Verpflichtung einer Behörde erforderlich ist, 6) mit Einwilligung der betroffenen Person zu der spezifischen Übermittlung von Daten, nachdem die betroffene Person zuvor über die Art der Verarbeitung unterrichtet wurde, erfolgt oder 7) wenn diese zur Erfüllung einer rechtlichen oder regulatorischen Verpflichtung, zur Erfüllung eines Vertrags oder zur Ausübung von Rechten in Gerichts-, Verwaltungs- oder Schiedsverfahren erforderlich ist¹⁶². Wie in der Datenübermittlungsverordnung festgelegt, können internationale Übermittlungen in diesen Fällen nur durchgeführt werden, wenn „die Besonderheiten des Einzelfalls und die geltenden rechtlichen Anforderungen erfüllt sind“¹⁶³.
- (111) In Bezug auf den bestimmten Fall, in dem die Datenübermittlung auf der Grundlage der Einwilligung der betroffenen Personen durchgeführt werden kann, ist es erforderlich, dass 1) die formalen Kriterien für die Erteilung einer gültigen Einwilligung erfüllt sind (d. h. die Einwilligung muss für den bestimmten Fall, freiwillig, ausdrücklich und in Kenntnis der Sachlage erteilt werden), 2) die betroffenen Personen über die Art der Übermittlung informiert werden, *bevor* diese durchgeführt wird (z. B. Informationen über die gerichtliche Zuständigkeit für die beabsichtigte Übermittlung und das dadurch garantierte Schutzniveau, Informationen über das Fehlen eines Angemessenheitsbeschlusses oder anderer Datenübermittlungsmechanismen, Informationen über die Dauer der Übermittlungen) und 3) die Einwilligung für jede Übermittlung einzeln und gesondert von jeder anderen Verarbeitung eingeholt wird. Wie in Erwägungsgrund 46 dargelegt, kann eine stillschweigende Zustimmung nicht als gültige Einwilligung angesehen werden, und die betroffenen Personen haben das Recht, ihre Einwilligung jederzeit zu widerrufen.
- (112) In der Datenübermittlungsverordnung ist die Verwendung all dieser Mechanismen streng an mehrere Bedingungen geknüpft. Dazu gehört insbesondere, dass der betroffenen Person „klare, sachlich richtige und leicht zugängliche Informationen über die Übermittlung“ zur Verfügung gestellt werden und dass gewährleistet wird und nachgewiesen werden kann, dass die internationalen Übermittlungen in einer Weise erfolgen, mit der die Einhaltung der Grundsätze und der Rechte der betroffenen Person sichergestellt und das im LGPD vorgesehene Schutzniveau nicht beeinträchtigt wird, „unabhängig davon, in welchem Land sich die personenbezogenen Daten, die Gegenstand der Übermittlung sind, befinden, und zwar auch nach Beendigung der Verarbeitung und im Falle einer Weiterübermittlung“¹⁶⁴. Diese Anforderungen gelten

¹⁶¹ Artikel 35 Absatz 4 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹⁶² Artikel 33 Ziffern III bis IX des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹⁶³ Artikel 1 (Hauptabsatz), ANPD, Verordnung über internationale Datenübermittlungen, August 2024.

¹⁶⁴ Artikel 2 Ziffern I und IV sowie Artikel 4, ANPD, Verordnung über internationale Datenübermittlungen, August 2024. Wie bei allen internationalen Übermittlungen erfolgt jede Übermittlung im Rahmen dieser Szenarien zu „berechtigten, spezifischen und eindeutigen Zwecken, die

auch für Übermittlungen auf der Grundlage „bestimmter Fälle“, um die Kontinuität des Schutzes unabhängig von dem zur Durchführung einer internationalen Übermittlung verwendeten Instrument sicherzustellen.

- (113) Durch die in den Erwägungsgründen 96 bis 112 dieses Beschlusses beschriebenen Vorschriften wird daher die Kontinuität des Schutzes bei der Weiterübermittlung personenbezogener Daten aus Brasilien in einer Weise gewährleistet, die im Wesentlichen den Bestimmungen der Verordnung (EU) 2016/679 entspricht.

2.4.12. Rechenschaftspflicht

- (114) Nach dem Grundsatz der Rechenschaftspflicht müssen Daten verarbeitende Unternehmen geeignete technische und organisatorische Maßnahmen treffen, um ihren Datenschutzpflichten wirksam nachzukommen und dies, insbesondere gegenüber der zuständigen Aufsichtsbehörde, nachweisen zu können.
- (115) In Artikel 6 Ziffer IX LGPD ist der Grundsatz der Rechenschaftspflicht festgelegt, wonach der Verantwortliche und der Auftragsverarbeiter Maßnahmen ergreifen müssen, die „effizient und geeignet“ sind, die Einhaltung des LGPD nachzuweisen.
- (116) Um die Rechenschaftspflicht zu gewährleisten, sieht Artikel 50 LGPD vor, dass Verantwortliche und Auftragsverarbeiter interne Vorschriften und Governance-Modelle einführen können, um insbesondere für bewährte Verfahren bei der Bearbeitung von Beschwerden und Anträgen von betroffenen Personen zu sorgen und die Sicherheitspflichten und alle anderen Verpflichtungen im Rahmen des LGPD einzuhalten („Bewährte Verfahren und Governance“). Diese Programme sollten auch Pläne für Schulungsmaßnahmen, interne Überwachungsmechanismen und Risikominderung umfassen.
- (117) Das LGPD sieht auch vor, dass ein Datenschutzbeauftragter (im Folgenden „DSB“) ernannt werden muss, dem eine wichtige Rolle bei der Gestaltung und Durchführung dieser internen Programme zukommt. Gemäß Artikel 5 Ziffer VIII dient der DSB als Bindeglied zwischen dem für die Verarbeitung Verantwortlichen, den betroffenen Personen und der ANPD. Gemäß Artikel 41 LGPD sind alle Verantwortlichen verpflichtet, einen DSB zu benennen und dessen Identität öffentlich bekannt zu geben.
- (118) Nach dem LGPD ist die ANPD ermächtigt, eine Ausnahme von der Verpflichtung für Verantwortliche und Auftragsverarbeiter zur Ernennung eines DSB zuzulassen¹⁶⁵. In ihrer Verordnung über die Anwendung des LGPD auf kleine und mittlere Unternehmen (im Folgenden „KMU“) hat die ANPD festgelegt, dass bestimmte Kleinstunternehmen, KMU, Start-up-Unternehmen und gemeinnützige Organisationen unter diese Ausnahme fallen können¹⁶⁶. Die Ausnahme gilt insbesondere für die folgenden Einrichtungen: „Kleinstunternehmen, kleine Unternehmen, Start-up-Unternehmen, juristische Personen des Privatrechts, einschließlich gemeinnütziger Organisationen, im Einklang mit den geltenden Rechtsvorschriften sowie natürliche Personen und anonymisierte private Einrichtungen, die personenbezogene Daten

der betroffenen Person mitgeteilt werden, ohne dass eine Weiterverarbeitung möglich ist, die mit diesen Zwecken unvereinbar ist“, wie in Artikel 9 Hauptabsatz der Verordnung über internationale Datenübermittlungen der ANPD vom August 2024 festgelegt.

¹⁶⁵ Artikel 41 Absatz 3 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹⁶⁶ ANPD, Verordnung über die Anwendung des LGPD auf kleine und mittlere Unternehmen (im Folgenden „Verordnung über KMU“, April 2024. Abrufbar unter: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022.

verarbeiten“¹⁶⁷. Nach brasilianischem Recht sind Kleinstunternehmen¹⁶⁸, kleine Unternehmen¹⁶⁹ oder Start-up-Unternehmen¹⁷⁰ Unternehmen mit einem einzigen oder einer geringen Anzahl von Beschäftigten¹⁷¹, deren jährliche Bruttoeinnahmen unter einem bestimmten Betrag liegen¹⁷².

- (119) Die Ausnahme von der Pflicht zur Ernennung eines DSB gilt nicht für Unternehmen und Einrichtungen, unabhängig von ihrer Größe oder ihren Einnahmen, die personenbezogene Daten „mit hohem Risiko“ verarbeiten¹⁷³. Eine Verarbeitung gilt als „mit hohem Risiko“ behaftet, wenn sie kumulativ mindestens eines der folgenden allgemeinen Merkmale aufweist: 1) Verarbeitung personenbezogener Daten in großem Umfang und 2) Verarbeitung von Daten, die erhebliche Auswirkungen auf die Grundrechte und Interessen der betroffenen Personen haben kann, sowie mindestens eines der folgenden besonderen Merkmale aufweist: 1) Einsatz neuer oder innovativer Technologien, 2) Überwachung oder Kontrolle von öffentlich zugänglichen Bereichen, 3) ausschließlich automatisierte Entscheidungsprozesse und 4) Verarbeitung sensibler Daten oder Daten von Kindern oder älteren Menschen¹⁷⁴. Eine Verarbeitung personenbezogener Daten „in großem Umfang“ ist definiert als eine Verarbeitung, die „eine erhebliche Anzahl betroffener Personen betrifft, auch unter Berücksichtigung des Datenvolumens sowie der Dauer, der Häufigkeit und des geografischen Umfangs der durchgeführten Verarbeitung“¹⁷⁵. Eine „Verarbeitung von Daten, die erhebliche Auswirkungen auf die Grundrechte und Interessen der betroffenen Personen haben kann“ wird definiert als „unter anderem Situationen, in denen die Verarbeitungstätigkeit die Ausübung von Rechten oder die Nutzung einer Dienstleistung behindern und für die betroffenen Personen materielle oder moralische Schäden wie Diskriminierung, Verletzung der körperlichen Unversehrtheit, des Rechts

¹⁶⁷ Artikel 2 Ziffer I, ANPD, Verordnung über KMU, April 2024.

¹⁶⁸ Ein „Kleinstunternehmen“ wird definiert als ein Unternehmen mit jährlichen Bruttoeinnahmen von höchstens 360 000 BRL (brasilianische Real). Siehe Artikel 3 Ziffer I des Ergänzungsgesetzes Nr. 123 vom 14. Dezember 2006, Gesetz über den nationalen Status von Kleinstunternehmen sowie kleinen und mittleren Unternehmen. 360 000 BRL entsprechen 56 500 EUR.

¹⁶⁹ Ein „kleines Unternehmen“ oder „KMU“ wird definiert als ein Unternehmen mit jährlichen Bruttoeinnahmen von mindestens 360 000 BRL und höchstens 4 800 000 BRL. Siehe Artikel 3 Ziffer II des Ergänzungsgesetzes Nr. 123 vom 14. Dezember 2006 über den nationalen Status von Kleinstunternehmen sowie kleinen und mittleren Unternehmen. 4 800 000 BRL entsprechen 753 000 EUR.

¹⁷⁰ „Start-up-Unternehmen“ werden definiert als „Unternehmen oder Unternehmensorganisationen, die neu gegründet wurden oder seit Kurzem tätig sind und deren Tätigkeiten durch Innovationen gekennzeichnet sind, die auf das Geschäftsmodell oder die angebotenen Produkte oder Dienstleistungen angewandt werden“. Siehe Artikel 2 Ziffer III, ANPD, Verordnung über KMU, April 2024.

Ein Start-up-Unternehmen kann nur für einen Zeitraum von höchstens zehn Jahren als solches registriert werden, wobei die jährlichen Bruttoeinnahmen auf 16 000 000 BRL begrenzt sind. Siehe Artikel 4 Ziffer I des Ergänzungsgesetzes Nr. 182 vom 1. Juni 2021, Gesetz über Start-up-Unternehmen. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp182.htm. 16 000 000 BRL entsprechen 2 500 000 EUR.

¹⁷¹ Siehe insbesondere Artikel 2 Ziffer II, ANPD, Verordnung über KMU, April 2024 und Artikel 41 des Gesetzes Nr. 14.195 vom 26. August 2021 über die Gründung von Unternehmen. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14195.htm.

¹⁷² Ergänzungsgesetz Nr. 123 vom 14. Dezember 2006 über den nationalen Status von Kleinstunternehmen sowie kleinen und mittleren Unternehmen. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp123.htm.

¹⁷³ Artikel 4, ANPD, Verordnung über KMU, April 2024.

¹⁷⁴ Artikel 4 Ziffern I und II, ANPD, Verordnung über KMU, April 2024.

¹⁷⁵ Siehe beispielsweise Artikel 4 Absatz 1, ANPD, Verordnung über KMU, April 2024.

am eigenen Bild und des guten Rufs, Finanzbetrug oder Identitätsdiebstahl verursachen kann“¹⁷⁶.

- (120) Die ANPD hat eine verbindliche Verordnung über die Rolle des Datenschutzbeauftragten (im Folgenden „DSB-Verordnung“) angenommen, in der dessen Aufgaben näher erläutert werden¹⁷⁷. In dieser Verordnung weist die ANPD darauf hin, dass private Einrichtungen und Behörden verpflichtet sind, Informationen über die Identität ihres Datenschutzbeauftragten zu veröffentlichen¹⁷⁸. In Artikel 10 der DSB-Verordnung wird darauf hingewiesen, dass die Verantwortlichen und Auftragsverarbeiter unter anderem verpflichtet sind, dafür zu sorgen, dass der DSB seine Aufgaben unabhängig und „ohne ungebührliche Einflussnahme, insbesondere bei der Beratung zu den im Zusammenhang mit dem Schutz personenbezogener Daten anzuwendenden Verfahren“ wahrnehmen kann und dass der DSB direkten Zugang zur höchsten Führungsebene und zu allen Beschäftigten erhält, die an strategischen Entscheidungen über die Verarbeitung von Daten innerhalb einer Einrichtung beteiligt sind. Ebenso hat der DSB seine Pflichten und Aufgaben mit „Ethik, Integrität und technischer Unabhängigkeit wahrzunehmen und Situationen zu vermeiden, die einen Interessenkonflikt darstellen könnten“¹⁷⁹.
- (121) Die Rolle des Datenschutzbeauftragten stellt eine Priorität der Durchsetzungsmaßnahmen der ANPD dar. So betrafen beispielsweise die ersten Sanktionen der ANPD ein Unternehmen, das mit einer Geldbuße belegt wurde und eine ausdrückliche Verwarnung erhielt, weil es nicht nachweisen konnte, dass es einen DSB ernannt hatte¹⁸⁰. Das Unternehmen beschloss während des Verwaltungsverfahrens, einen DSB zu benennen, um der Anordnung der ANPD nachzukommen. Seitdem hat die ANPD weiterhin Sanktionen gegen öffentliche und private Einrichtungen im Zusammenhang mit den im Rahmen des LGPD festgelegten Bestimmungen zum DSB verhängt¹⁸¹.
- (122) Die Datenschutz-Folgenabschätzung ist ein weiteres wichtiges Instrument zur Gewährleistung der Rechenschaftspflicht. Mit einer Datenschutz-Folgenabschätzung können die Auswirkungen einer Verarbeitung bewertet und bestimmt werden. Nach Artikel 38 LGPD kann die ANPD einen Verantwortlichen oder Auftragsverarbeiter auffordern, eine Datenschutz-Folgenabschätzung zu erstellen¹⁸², die eine Beschreibung der Art der Verarbeitung der personenbezogenen Daten sowie Maßnahmen, Schutzvorkehrungen und Mechanismen zur Risikominderung enthalten muss. Darüber hinaus enthält Abschnitt II des LGPD Bestimmungen über die Rechenschaftspflicht, mit denen die ANPD ermächtigt wird, die Veröffentlichung einer Datenschutz-

¹⁷⁶ Siehe beispielsweise Artikel 4 Absatz 2, ANPD, Verordnung über KMU, April 2024.

¹⁷⁷ ANPD, Verordnung über die Rolle des Datenschutzbeauftragten bei der Verarbeitung personenbezogener Daten (im Folgenden „DSB-Verordnung“), Juli 2024. Abrufbar unter: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074>.

¹⁷⁸ Artikel 5 und 9, ANPD, DSB-Verordnung, Juli 2024.

¹⁷⁹ Artikel 18, ANPD, DSB-Verordnung, Juli 2024.

¹⁸⁰ Siehe ANPD, Bericht über die Dienstanweisung Nr. 1/2023 – Telekall Infoservice. Abrufbar unter: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforsevice.pdf.

¹⁸¹ Siehe z. B. ANPD, Bericht über die Dienstanweisung Nr. 5/2024 – Ministério da Saúde. Abrufbar unter: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/deciso-es-em-processos-sancionadores-1/relatorio_de_instrucao_5_publico_ocultado.pdf.

¹⁸² Artikel 38 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

Folgenabschätzung zu verlangen oder die Annahme „bewährter Verfahren“ zum Schutz personenbezogener Daten durch Behörden zu empfehlen¹⁸³.

- (123) Angesichts der in den Erwägungsgründen 114 bis 122 dieses Beschlusses beschriebenen Rechenschaftspflichten und -praktiken setzt der brasilianische Rechtsrahmen den Grundsatz der Rechenschaftspflicht in ähnlicher Weise um wie die in Kapitel 4 Abschnitte 3 und 4 der Verordnung (EU) 2016/679 vorgesehenen Maßnahmen, unter anderem indem verschiedene Mechanismen vorgesehen werden, um die Einhaltung des LGPD sicherzustellen und nachzuweisen.

2.5. Aufsicht und Durchsetzung

- (124) Um sicherzustellen, dass in der Praxis ein angemessenes Datenschutzniveau gewährleistet ist, sollte eine unabhängige Aufsichtsbehörde mit der Befugnis zur Überwachung und Durchsetzung der Einhaltung der Datenschutzvorschriften eingerichtet werden. Diese Behörde sollte bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse vollkommen unabhängig und unparteiisch handeln.

2.5.1. Unabhängige Aufsicht

- (125) In Brasilien ist die für die Überwachung und Durchsetzung des LGPD zuständige unabhängige Aufsichtsbehörde die Agência Nacional de Proteção de Dados – ANPD.
- (126) Die ANPD wurde durch Artikel 55-A LGPD geschaffen und bildet eine unabhängige Stelle, zunächst durch einen vorläufigen Erlass und dann durch ein Gesetz im Jahr 2022¹⁸⁴. Mit der Verabschiedung des Gesetzes zur Umgestaltung der ANPD wurde das LGPD geändert, um Bestimmungen aufzuheben, mit denen die Funktionsweise und die Finanzoperationen der ANPD von Genehmigungen abhängig waren, die von der Exekutive nach dem brasilianischen Haushaltsgesetz erteilt werden mussten¹⁸⁵. In der geänderten Bestimmung des LGPD wird anerkannt, dass die ANPD eine „Sonderbehörde mit technischer und Entscheidungsautonomie, mit eigenem Vermögen und mit Sitz im Bundesdistrikt“ ist¹⁸⁶.
- (127) Als „Behörde mit Sonderstatus“ verfügt die ANPD über die Autonomie, ihre im LGPD festgelegten rechtlichen Aufgaben und Befugnisse, einschließlich der Verwaltung der Agentur, in vollem Umfang wahrzunehmen¹⁸⁷. Dies schließt die

¹⁸³ Abschnitt II des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹⁸⁴ Artikel 55-A des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), in seiner ursprünglichen Fassung, wurde durch das Gesetz Nr. 14.460 vom 25. Oktober 2022 geändert, mit dem die ANPD in eine Behörde mit Sonderstatus umgewandelt wurde. Zur Unabhängigkeit siehe die vorläufige Maßnahme Nr. 1.124 vom 13. Juni 2022, mit der die ANPD in eine Behörde mit Sonderstatus umgewandelt wurde. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Mpv/mpv1124.htm und Gesetz Nr. 14.460 vom 25. Oktober 2022 zur Umwandlung der ANPD in eine Behörde mit Sonderstatus. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Lei/L14460.htm. Die Möglichkeit für die Regierung, den Status der ANPD zu ändern, um deren Unabhängigkeit zu erhöhen, wurde in (dem mittlerweile aufgehobenen) Artikel 55-A Absatz 1 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz, geregelt.

¹⁸⁵ Siehe Artikel 9 des Gesetzes Nr. 14.460 vom 25. Oktober 2022 zur Umwandlung der ANPD in eine Behörde mit Sonderstatus, mit dem Artikel 55-A des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz, aufgehoben und ersetzt wurde.

¹⁸⁶ Artikel 7 des Gesetzes Nr. 14.460 vom 25. Oktober 2022 zur Umwandlung der ANPD in eine Behörde mit Sonderstatus.

¹⁸⁷ Siehe ANPD, Die ANPD wird zu einer Sonderbehörde, Juni 2022. Abrufbar unter: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-autarquia-de-natureza-especial>.

Autonomie bei der Verwaltung der Ausgaben und bei Einstellungen ein¹⁸⁸. Die ANPD wurde zunächst als „Behörde“ eingerichtet, bevor sie im September 2025 in eine „Agentur“ umgewandelt wurde, wodurch ihr Name mit elf weiteren Regulierungsstellen in Einklang gebracht wurde, die in Brasilien über ein solch hohes Maß an Unabhängigkeit verfügen (z. B. die Nationale Agentur für Elektrizität, die Nationale Agentur für Telekommunikation usw.)¹⁸⁹.

- (128) Die Mittel der ANPD stammen weitgehend aus dem allgemeinen Haushalt Brasiliens. Darüber hinaus kann der Haushalt der ANPD Spenden, Zuschüsse oder andere Kredite gemäß Artikel 55-L LGPD umfassen. Seit ihrer Gründung im Jahr 2021 ist die ANPD exponentiell gewachsen. Aus Jahresberichten der ANPD geht hervor, dass die Behörde nach nur vierjährigem Bestehen Ende 2023 141 Mitarbeiter/Beamte beschäftigte¹⁹⁰. Das jährliche Budget der ANPD für das Jahr 2025 beläuft sich auf 18 Mio. BRL¹⁹¹. Im September 2025 wurde in Brasilien die Schaffung einer neuen Laufbahn im öffentlichen Dienst zum Thema „Datenschutz“ mit 200 Stellen bekannt gegeben, die Teil einer Aufstockung der Belegschaft der ANPD in den kommenden Jahren sein soll¹⁹².
- (129) Die ANPD besteht aus einem Verwaltungsrat (dem höchsten Leitungsgremium), einem Nationalen Rat für den Schutz personenbezogener Daten und der Privatsphäre (mit beratender Funktion) und mehreren Verwaltungsstellen und -referaten¹⁹³. Diese Struktur ist in Artikel 55-C LGPD festgelegt und wird in zwei Verordnungen, die 2020 bzw. 2023 angenommen wurden, näher ausgeführt¹⁹⁴.
- (130) Der Verwaltungsrat setzt sich aus fünf Verwaltungsratsmitgliedern zusammen, zu denen auch der Präsident der Behörde gehört. Jedes Mitglied des Verwaltungsrats der ANPD wird vom Präsidenten der Republik Brasilien nach Zustimmung des Bundessenats für fünf Jahre ernannt¹⁹⁵.

¹⁸⁸ Artikel 55-L des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹⁸⁹ Artikel 1 des Erlasses Nr. 1.317 vom 17. September 2025 zur Änderung des LGPD zwecks Umgestaltung der ANPD. Abrufbar unter: <https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314> und Artikel 2 Ziffer XII des Gesetzes Nr. 13.848 vom 25. Juni 2019 über die Organisation der Regulierungsagenturen. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/113848.htm.

¹⁹⁰ ANPD, Bericht über das vierte Tätigkeitsjahr der ANPD, November 2023, S. 8. Abrufbar unter: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/balanco-de-4-anos-anpd-2024.pdf/view>.

¹⁹¹ 18 225 566 BRL (2 857 768 EUR). Siehe Jährliches Haushaltsgesetz, S. 190. Abrufbar unter: LEI15121-VOLUME I.pdf.

¹⁹² Artikel 9 Ziffer I des Erlasses Nr. 1.317 vom 17. September 2025 zur Änderung des LGPD zwecks Umgestaltung der ANPD. Abrufbar unter: <https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314>.

¹⁹³ Artikel 55-C des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹⁹⁴ Erlass Nr. 10.474 vom 26. August 2020 über die Struktur der ANPD. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm, geändert durch Erlass Nr. 11.758 vom 30. Oktober 2023 über die geänderte Struktur der ANPD. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11758.htm#art1.

¹⁹⁵ Artikel 55-D Absätze 1 und 3 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz – und Artikel 12 des Erlasses Nr. 1.317 vom 17. September 2025 zur Änderung des LGPD zwecks Umgestaltung der ANPD. Abrufbar unter: <https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314>. In Artikel 12 dieses Erlasses wird die Dauer des Mandats der Verwaltungsratsmitglieder der ANPD von vier auf fünf Jahre verlängert, um eine Angleichung an alle anderen unabhängigen Regulierungsagenturen in Brasilien vorzunehmen. Alle Verwaltungsratsmitglieder der ANPD, die vor

- (131) Die Mitglieder des Verwaltungsrats müssen brasilianische Staatsangehörige sein und über ein hohes Bildungsniveau, das für die Stelle relevant ist, verfügen¹⁹⁶. Um ihre Unabhängigkeit zu gewährleisten, müssen alle Mitglieder des Verwaltungsrats u. a. von gewinnorientierten und politischen Tätigkeiten sowie von Führungs- oder Beratungspositionen in Unternehmen absehen¹⁹⁷. Darüber hinaus sieht das brasilianische Gesetz zur Regelung der Ausübung leitender Positionen in der öffentlichen Bundesverwaltung vor, dass es natürlichen Personen, die Funktionen ausüben, die denen der Verwaltungsratsmitglieder der ANPD gleichwertig sind, unter anderem verboten ist, Tätigkeiten auszuüben, die mit ihren Aufgaben unvereinbar sind¹⁹⁸. Dazu gehört auch die Tätigkeit als Berater oder Vermittler privater Interessen (auch informell) oder die Erbringung von Dienstleistungen für Einrichtungen, die der Aufsicht oder Regulierung der ANPD unterliegen, selbst wenn dies nur gelegentlich geschieht. Darüber hinaus ist es den Mitgliedern des Verwaltungsrats am Ende ihres Mandats oder ihrer Amtszeit bei der ANPD und für einen Zeitraum von sechs Monaten danach untersagt, bestimmte Funktionen auszuüben, die zu Interessenkonflikten führen könnten¹⁹⁹.
- (132) Mitglieder des Verwaltungsrats können nur unter bestimmten, in Artikel 55-E LGPD definierten Umständen entlassen werden, nämlich „bei Rücktritt, rechtskräftiger und unanfechtbarer gerichtlicher Verurteilung oder Entlassung aufgrund eines disziplinarischen Verwaltungsverfahrens“. Im Bundesgesetz über öffentliche Ämter ist festgelegt, dass eine solche Sanktion gerechtfertigt sein muss und nur bei nachgewiesenen konkreten Verstößen (z. B. schwerwiegendes Fehlverhalten, Korruption, unrechtmäßige Verwendung öffentlicher Mittel) vorgeschlagen werden kann²⁰⁰. Diese Regeln und Verfahren bieten den Verwaltungsratsmitgliedern der ANPD einen institutionellen Schutz bei der Wahrnehmung ihrer Aufgaben. Bislang wurden weder Verwaltungsratsmitglieder der ANPD entlassen noch Disziplinarverfahren eingeleitet. Der Verwaltungsrat der ANPD ist seit seiner Einsetzung unverändert geblieben, auch nach dem Regierungswechsel in Brasilien im Jahr 2023.
- (133) Die Aufgaben und Befugnisse der ANPD sind in Artikel 55-J LGPD festgelegt. Sie umfassen insbesondere die Entwicklung von Datenschutzstrategien und -leitlinien, die Förderung der Einführung von Standards, die den betroffenen Personen die Kontrolle über ihre personenbezogenen Daten erleichtern, die Untersuchung von Verletzungen individueller Rechte, die Bearbeitung von Beschwerden, die Durchsetzung der Einhaltung des LGPD und die Verhängung von Sanktionen, die Gewährleistung von

der Verabschiedung dieses Erlasses benannt wurden, werden gemäß den zum Zeitpunkt ihrer Ernennung geltenden gesetzlichen Vorschriften ihr Mandat für vier Jahre ausüben.

¹⁹⁶ Artikel 55-D Absatz 2 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

¹⁹⁷ Artikel 11 des Erlasses Nr. 10.474 vom 26. August 2020 über die Struktur der ANPD.

¹⁹⁸ Artikel 5 des Gesetzes Nr. 12.813 vom 16. Mai 2013 über Interessenkonflikte für Beamte und andere Positionen in der öffentlichen Verwaltung. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12813.htm.

¹⁹⁹ Artikel 6 des Gesetzes Nr. 12.813 vom 16. Mai 2013 über Interessenkonflikte für Beamte und andere Positionen in der öffentlichen Verwaltung.

²⁰⁰ Die vollständige und erschöpfende Liste der Verstöße findet sich in Artikel 132 des Gesetzes Nr. 8112 vom 11. Dezember 1990, Bundesgesetz über öffentliche Ämter und Beamte. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm. Siehe auch Kapitel V dieses Gesetzes über die Voraussetzungen für die Verhängung einer Sanktion.

Aufklärung und Förderung im Bereich des Datenschutzes sowie den Austausch und die Zusammenarbeit mit Datenschutzbehörden von Drittländern²⁰¹.

- (134) Die ANPD verfügt über ein beratendes Gremium, das vom Nationalen Rat für den Schutz personenbezogener Daten und der Privatsphäre gemäß Artikel 58-A LGPD gebildet wird. Dieses Gremium setzt sich aus Vertretern der Exekutive, der Legislative und der Judikative sowie der Zivilgesellschaft, der Gewerkschaften und der Wirtschaft zusammen²⁰². Es hat eine rein beratende Funktion, und seine Aufgabe besteht darin besteht, Studien oder Jahresberichte zum Thema Datenschutz auszuarbeiten, öffentliche Aussprachen und Anhörungen zum Schutz personenbezogener Daten und der Privatsphäre durchzuführen, der ANPD unverbindliche Empfehlungen zu unterbreiten und Wissen über den Schutz personenbezogener Daten und der Privatsphäre zu verbreiten²⁰³. Bei der Zusammenarbeit zwischen der ANPD und dem Nationalen Rat steht die Förderung des Datenschutzes und der Privatsphäre in Brasilien im Mittelpunkt. Der Nationale Rat hat keine Befugnisse in Bezug auf die Überwachung und Durchsetzung des LGPD, denn nur die ANPD ist befugt, die Umsetzung des Gesetzes zu überwachen und es durchzusetzen, z. B. durch den Erlass von Verordnungen, die Durchführung von Untersuchungen und die Verhängung von Sanktionen. Als unabhängige Behörde ist die ANPD nicht verpflichtet, den Vorschlägen zu folgen, die der Nationale Rat in seinen Berichten oder unverbindlichen Empfehlungen unterbreitet.

2.5.2. Durchsetzung, einschließlich Sanktionen

- (135) Um die Einhaltung der Vorschriften durchzusetzen, hat der Gesetzgeber der ANPD sowohl Untersuchungs- als auch Durchsetzungsbefugnisse übertragen, die von Verwarnungen bis hin zu Geldbußen reichen.
- (136) In Bezug auf Untersuchungsbefugnisse kann die ANPD, wenn ein Verstoß gegen das LGPD vermutet wird oder gemeldet wurde oder wenn dies für den Schutz der Rechte betroffener Personen, die verletzt wurden oder mutmaßlich verletzt werden, erforderlich ist, jederzeit Prüfungen und Vor-Ort-Kontrollen bei Verantwortlichen aus dem öffentlichen und privaten Sektor durchführen und alle erforderlichen Informationen anfordern²⁰⁴. Insbesondere sieht die verbindliche Verordnung über die Sanktionsbefugnisse der ANPD vor, dass die Verantwortlichen und Auftragsverarbeiter der ANPD „den Zugang zu Büros/Gebäuden, Ausrüstung, Anwendungen, Einrichtungen, Systemen, Tools und technologischen Ressourcen, Dokumenten, Daten und Informationen technischer, operativer und sonstiger Art, die für die Beurteilung der Verarbeitung personenbezogener Daten von Bedeutung sind und sich in ihrem Besitz oder im Besitz Dritter befinden“, gewähren müssen²⁰⁵.

²⁰¹ Artikel 55-J Ziffern I bis XXIV des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

²⁰² Für weitere Informationen über die Mitglieder und Tätigkeiten des Nationalen Rats siehe ANPD, Nationaler Rat für den Schutz personenbezogener Daten und der Privatsphäre. Abrufbar unter: <https://www.gov.br/anpd/pt-br/cnpd-2>.

²⁰³ Artikel 58-B des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

²⁰⁴ Artikel 55-J Ziffer XVI des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Artikel 4 Ziffer I des Erlasses Nr. 10.474 vom 26. August 2020 über die Struktur der ANPD und Artikel 12, ANPD, Verordnung über die Meldung von Sicherheitsvorfällen, April 2024.

²⁰⁵ Artikel 5, ANPD, Verordnung über die Sanktionsbefugnisse der ANPD, Oktober 2021. Abrufbar unter: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no1-2021.

- (137) Im Rahmen ihrer Abhilfebefugnisse kann die ANPD Verwarnungen, Geldbußen oder andere Sanktionen verhängen, z. B. Anordnungen, die Verarbeitung von Daten vorübergehend einzustellen oder personenbezogene Daten zu löschen²⁰⁶. Diese Sanktionen können gegen öffentliche oder private Einrichtungen verhängt werden, mit Ausnahme von Geldbußen und Tagessätzen, die nicht gegen öffentliche Einrichtungen verhängt werden können²⁰⁷. Es können mehrere kumulative Sanktionen verhängt werden, um eine Einrichtung zur Einhaltung der Vorschriften zu bewegen. Im Wege einer Verwarnung würde die ANPD einem Verantwortlichen eine bestimmte Frist setzen, innerhalb derer er Abhilfemaßnahmen ergreifen muss, um die Verarbeitung mit dem LGPD in Einklang zu bringen²⁰⁸. Die Nichterfüllung dieser Verpflichtung würde zu zusätzlichen Sanktionen führen. So hat die ANPD beispielsweise mehrere Verwarnungen an das Gesundheitsministerium gerichtet, weil dieses unter anderem keine Datenschutz-Folgenabschätzung vorgelegt und eine Datenschutzverletzung nicht gemeldet hatte²⁰⁹. Die ANPD kann verschiedene Sanktionen miteinander verknüpfen, um die Rechte der betroffenen Personen zu schützen oder die Einhaltung des LGPD sicherzustellen. So kann die ANPD beispielsweise bei einem Verstoß gegen das LGPD eine Geldbuße verhängen und gleichzeitig die Löschung von Daten, die mit diesem Verstoß in Verbindung stehen, anordnen²¹⁰. Die ANPD kann bei nicht finanziellen Sanktionen auch beschließen, „Tagessätze“ zu verhängen, „wenn dies erforderlich ist, um die Einhaltung (des LGPD) innerhalb einer Frist sicherzustellen“²¹¹. Die Tagessätze werden kumulativ unter Berücksichtigung der Zeitspanne zwischen dem Verhängen der Geldbuße und der Erfüllung der Verpflichtung bis zu einem Höchstbetrag von 50 Mio. BRL verhängt²¹².
- (138) Nach Artikel 52 Ziffer II LGPD kann die ANPD zusätzlich zu den Tagessätzen Geldbußen in Höhe von bis zu 2 % der Einnahmen eines Unternehmens in Brasilien verhängen, höchstens jedoch 50 Mio. BRL²¹³. Bei mehrfachen Verstößen können Geldbußen kumulativ verhängt werden. Die ANPD verhängte ihre ersten Geldbußen wenige Monate nach der Annahme der Verordnung über Sanktionen gegen ein Telekommunikationsunternehmen, das keine Rechtsgrundlage für die Verarbeitung angegeben und keinen Datenschutzbeauftragten benannt hatte. Das Unternehmen erhielt eine Verwarnung und zwei Geldbußen in Höhe von insgesamt 14 400 BRL²¹⁴. In der verbindlichen Verordnung über Sanktionen hat die ANPD die Sanktionen in drei Schweregrade eingeteilt: leicht, mittel und schwerwiegend²¹⁵, abhängig von

²⁰⁶ Artikel 55 und 55-J Ziffer IV des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) und ANPD, Verordnung über Sanktionen, Februar 2023.

²⁰⁷ Artikel 52 Absatz 3. Gesetz Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

²⁰⁸ Artikel 52 Ziffer I des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

²⁰⁹ Siehe ANPD, Beschluss Nr. 4/2024, abrufbar unter https://www.gov.br/anpd/pt-br/centrais-de-contenido/relatorio_de_instrucao_no_4_2024_fis_cgf_anpd_v-publica.pdf und ANPD, Beschluss Nr. 5/2024, abrufbar unter: https://www.gov.br/anpd/pt-br/centrais-de-contenido/deciso-es-em-processos-sancionadores-1/relatorio_de_instrucao_5_publico_ocultado.pdf.

²¹⁰ Artikel 52 Ziffer VI des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

²¹¹ Artikel 16, ANPD, Verordnung über Sanktionen, Februar 2023.

²¹² Artikel 16 Absatz 1, ANPD, Verordnung über Sanktionen, Februar 2023. 50 Mio. BRL entsprechen rund 7,8 Mio. EUR.

²¹³ 50 Mio. BRL entsprechen rund 7,8 Mio. EUR.

²¹⁴ ANPD, Beschluss Nr. 1/2023, abrufbar unter: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_infor-service.pdf.

²¹⁵ Artikel 8, ANPD, Verordnung über Sanktionen, Februar 2023.

festgelegten Faktoren wie Art und Umfang der verarbeiteten Daten, Art der Verarbeitung oder Auswirkungen auf die Rechte der betroffenen Personen. So unterliegen beispielsweise Verstöße im Zusammenhang mit der Verarbeitung sensibler personenbezogener Daten den höchsten Sanktionen, die die ANPD verhängen kann²¹⁶.

- (139) Die Verordnung über Sanktionen sieht eine Methode für die Berechnung von Geldbußen vor, unter anderem zur Berücksichtigung erschwerender und/oder mildernder Umstände²¹⁷. So kann beispielsweise eine Geldbuße bei wiederholten spezifischen Verstößen um 10 % oder sogar um 90 % für jede nicht fristgerecht umgesetzte Abhilfemaßnahme erhöht werden²¹⁸. Ebenso kann eine Geldbuße um 50 % gemindert werden, wenn der Verstoß unmittelbar nach Einleitung des Verwaltungsverfahrens durch die ANPD behoben wird²¹⁹.
- (140) Das brasilianische System kombiniert daher verschiedene Arten von Sanktionen, von Abhilfemaßnahmen bis zu Geldbußen. Unmittelbar nach Inkrafttreten ihrer Sanktionsbefugnisse begann die ANPD, von diesen Gebrauch zu machen²²⁰. Bislang wurden sowohl gegen Behörden, auch im Bereich der Sicherheit, als auch gegen private Betreiber Sanktionen und Empfehlungen ausgesprochen²²¹. Die von der ANPD bislang verhängten Sanktionen betreffen ein breites Spektrum von Themen, darunter die fehlende Benennung eines Datenschutzbeauftragten, Sicherheitsvorfälle, einschließlich Datenschutzverletzungen, oder die mangelnde Zusammenarbeit mit der ANPD. Neben der Verhängung von Geldbußen hat die ANPD insbesondere die gesamte Bandbreite ihrer Abhilfebefugnisse genutzt, um beispielsweise den Verantwortlichen anzuordnen, eine Datenschutz-Folgenabschätzung durchzuführen oder die Verarbeitung personenbezogener Daten einzustellen. So erließ die ANPD beispielsweise im Juli 2024 eine Anordnung an eine große Social-Media-Plattform, die Verarbeitung personenbezogener Daten für die Schulung generativer künstlicher Intelligenz-Systeme bei sämtlichen Produkten auszusetzen²²². Zusammen mit dieser Präventivmaßnahme zum Schutz der Grundrechte betroffener Personen verhängte die ANPD Tagessätze in Höhe von 50 000 BRL, bis die Verarbeitung der Daten mit dem LGPD in Einklang gebracht wurde²²³. Schließlich kündigte die ANPD die Einleitung von Untersuchungen gegen mehrere große multinationale Technologieplattformen, Social-Media-Unternehmen und eine Bank an und setzte gleichzeitig die Untersuchungen gegen Einrichtungen des öffentlichen Sektors fort²²⁴. In den wenigen

²¹⁶ Artikel 8 Absatz 3, Ziffer I Buchstabe d, ANPD, Verordnung über Sanktionen, Februar 2023.

²¹⁷ Anhang I, Artikel 12-13, ANPD, Verordnung über Sanktionen, Februar 2023.

²¹⁸ Artikel 12 Ziffern I bis IV, ANPD, Verordnung über Sanktionen, Februar 2023.

²¹⁹ Artikel 13 Ziffer I, ANPD, Verordnung über Sanktionen, Februar 2023.

²²⁰ ANPD, Sanktionsregister. Abrufbar unter: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/deciso-es-em-processos-sancionadores-1/deciso-es-em-processos-sancionadores?_authenticator=7951f0a70d3d125fd05e11a1e544b72d2c61f304.

²²¹ Siehe beispielsweise Technischer Vermerk Nr. 175/2023 zum Entwurf eines Kooperationsabkommens zwischen dem Ministerium für Justiz und öffentliche Sicherheit und dem brasilianischen Fußballverband über den Austausch personenbezogener Daten im Hinblick auf die Verbesserung des Projekts „Sichere Stadien“. Abrufbar unter: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mj-sp-e-cbf.pdf>.

²²² ANPD, Präventivmaßnahme, Abstimmung Nr. 11/2024. Abrufbar unter: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta/SEI_0130047_Voto_11.pdf.

²²³ 50 000 BRL entsprechen 7 800 EUR.

²²⁴ Die vollständige und aktualisierte Liste der laufenden Untersuchungen und der von der ANPD eingeleiteten Verfahren ist abrufbar unter: <https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-de-fiscalizacao>.

Jahren ihres Bestehens hat die ANPD eine solide Erfolgsbilanz bei der Durchsetzung gezeigt und dabei ihre gesamten Durchsetzungsbefugnisse ausgeschöpft.

- (141) Schließlich ersetzen die im LGPD festgelegten Verwaltungssanktionen nicht die Anwendung anderer verwaltungsrechtlicher oder sonstiger zivil- und strafrechtlicher Sanktionen, einschließlich jener, die im brasilianischen Verbraucherschutzgesetz²²⁵ und im Zivilrechtlichen Rahmenwerk für das Internet²²⁶ festgelegt sind. Unternehmen sind nach dem brasilianischen Verbraucherschutzgesetz insbesondere verpflichtet, den Verbrauchern Informationen über ihre Unternehmen und Tätigkeiten zur Verfügung zu stellen²²⁷. In Artikel 56 des Verbraucherschutzgesetzes sind ferner die Sanktionen aufgeführt, die Unternehmen bei Verstößen drohen und von Geldbußen über ein Verbot des Verkaufs oder der Herstellung eines Produkts bis hin zur Verpflichtung zur Einstellung einer Dienstleistung reichen. Ferner sind in den Artikeln 61 bis 74 des Verbraucherschutzgesetzes die Straftaten aufgeführt, für die Unternehmen mit Freiheitsstrafen von sechs Monaten bis zu zwei Jahren rechnen müssen, auch im Falle falscher oder irreführender Angaben in Bezug auf eine Dienstleistung oder die Werbung für eine Dienstleistung, die dem Verbraucher schaden könnte. So verhängte beispielsweise das brasilianische Ministerium für Verbraucherschutz im Jahr 2014 Geldbußen in Höhe von 3,5 Mio. BRL gegen ein Telekommunikationsunternehmen wegen Verstößen gegen das Verbraucherschutzgesetz und das Zivilrechtliche Rahmenwerk für das Internet im Zusammenhang mit der Nutzung von Tracking für verhaltensorientierte Online-Werbung und dem Verkauf von Browsing-Daten²²⁸.
- (142) Daraus folgt, dass das brasilianische System eine wirksame Durchsetzung seiner Datenschutzvorschriften in der Praxis gewährleistet.

2.5.3. Rechtsbehelfe

- (143) Um einen angemessenen Schutz und insbesondere die Durchsetzung der Rechte des Einzelnen zu gewährleisten, sollten der betroffenen Person wirksame behördliche und gerichtliche Rechtsmittel, einschließlich der Möglichkeit einer Schadenersatzforderung, zur Verfügung stehen.
- (144) Das brasilianische System stellt dem Einzelnen verschiedene Mechanismen zur Verfügung, um seine Rechte wirksam durchzusetzen und Rechtsmittel geltend zu machen.
- (145) Natürliche Personen, die der Ansicht sind, dass ihre Datenschutzrechte oder -interessen verletzt wurden, oder die ihre Datenschutzrechte ausüben möchten, können sich in einem ersten Schritt an den jeweiligen Verantwortlichen wenden. Gemäß Artikel 9 LGPD stellt der für die Verarbeitung Verantwortliche unter anderem die Kontaktdaten zur Verfügung, die die Einreichung von Anträgen und „Schriftsätzen“ der betroffenen Personen ermöglichen²²⁹.
- (146) Darüber hinaus stehen natürlichen Personen, die der Ansicht sind, dass ihre Datenschutzrechte oder -interessen durch den Verantwortlichen oder den

²²⁵ Gesetz Nr. 8.079 vom 11. September 1990, Verbraucherschutzgesetz. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm.

²²⁶ Gesetz Nr. 12.965 vom 23. April 2014, Marco Civil da Internet („Zivilrechtliches Rahmenwerk für das Internet“). Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm.

²²⁷ Artikel 6 des Gesetz Nr. 8.079 vom 11. September 1990, Verbraucherschutzgesetz.

²²⁸ 3,5 Mio. BRL betragen auf der Grundlage des damaligen Wechselkurses rund 1,5 Mio. EUR.

²²⁹ Artikel 9 in Verbindung mit Artikel 55-J Ziffer V des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

Auftragsverarbeiter personenbezogener Daten verletzt wurden, gemäß LGPD und dem brasilianischen Rechtssystem mehrere Rechtsmittel zur Verfügung.

- (147) Erstens kann jede natürliche Person, die der Ansicht ist, dass ihre Datenschutzrechte oder -interessen durch den Verantwortlichen oder Auftragsverarbeiter verletzt wurden, Beschwerde bei der ANPD einreichen oder einen solchen Verstoß melden²³⁰. Die ANPD verfügt auf ihrer Webseite über eine eigene Seite, auf der betroffene Personen im Falle eines Verstoßes gegen das LGPD eine Beschwerde oder eine Petition im Zusammenhang mit einem an einen Verantwortlichen gerichteten Antrag hinsichtlich ihrer Datenschutzrechte einreichen können²³¹. Wie in Erwägungsgrund 138 dieses Beschlusses erläutert, kann die ANPD als Reaktion auf eine Beschwerde eine Sanktion gemäß Artikel 52 LGPD verhängen. Mit der Verordnung über die Sanktionsbefugnisse der ANPD wurde das Verwaltungsverfahren für ihre Verfahren festgelegt, einschließlich Fristen, Verfahren zur Regelung des Anspruchs auf rechtliches Gehör und Veröffentlichung der Entscheidung²³².
- (148) Die Entscheidungen der ANPD können von den betroffenen Personen angefochten werden, indem sie innerhalb von zehn Tagen nach Eingang der Entscheidungen beim Verwaltungsrat der ANPD Beschwerde einlegen²³³. Im Rahmen ihres Rechts auf einen wirksamen Rechtsbehelf können natürliche Personen die Entscheidungen des Verwaltungsrats vor Gericht anfechten sowie auch Rechtsbehelfe gegen Entscheidungen der ANPD einlegen, wenn diese ihren Verpflichtungen aus dem LGPD (einschließlich der Weigerung, eine Beschwerde zu bearbeiten, oder der Ablehnung einer Beschwerde in der Sache) nicht nachkommt²³⁴.
- (149) Zweitens kann die ANPD eine „direkte Schlichtung“ (Mediation) zwischen betroffenen Personen und Verantwortlichen fördern, um der Problemlösung und dem „Schadenersatz durch den Verantwortlichen“ Vorrang einzuräumen²³⁵. Diese Verfahren hindern die betroffenen Personen nicht daran, Beschwerden einzureichen oder andere Rechtsmittel in Anspruch zu nehmen.
- (150) Drittens verpflichtet Artikel 42 LGPD einen Verantwortlichen oder Auftragsverarbeiter, „materielle, immaterielle, individuelle oder kollektive Schäden Dritter“, die sich aus der Verarbeitung personenbezogener Daten ergeben, zu ersetzen. Betroffene Personen können einzeln oder kollektiv Klage erheben, um Abhilfe und Ersatz für diese Schäden zu verlangen²³⁶. Im LGPD ist festgelegt, dass es im Ermessen eines Richters liegt, „die Beweislast zugunsten der betroffenen Person umzukehren“, insbesondere in Fällen, in denen „die Vorlage von Beweisen durch die betroffene Person mit einem übermäßigen Aufwand verbunden wäre“²³⁷.

²³⁰ Artikel 55-J Ziffer V des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

²³¹ Siehe ANPD, Dienstleistungen für betroffene Personen, Einreichung einer Beschwerde oder Petition. Abrufbar unter: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/denuncia-peticao-de-titular.

²³² Abschnitte II und III, ANPD, Verordnung über die Sanktionsbefugnisse der ANPD, Oktober 2021.

²³³ Artikel 59, ANPD, Verordnung über die Sanktionsbefugnisse der ANPD, Oktober 2021.

²³⁴ Artikel 22 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

²³⁵ Artikel 17 Ziffer VIII, ANPD, Verordnung über die Sanktionsbefugnisse der ANPD, Oktober 2021.

²³⁶ Artikel 42 Absatz 3 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

²³⁷ Artikel 42 Absatz 2 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

- (151) Viertens gilt der in diesem Bereich gewährte Schutz, wenn eine Verletzung der Rechte betroffener Personen in den Anwendungsbereich des Verbraucherrechts und der Verbraucherbeziehungen fällt, und kann vor Gericht geltend gemacht werden²³⁸.
- (152) Fünftens hat das Oberste Bundesgericht Brasiliens anerkannt, dass natürliche Personen das Recht haben, Unterlassungsansprüche geltend zu machen, wenn ihre verfassungsmäßigen Rechte, einschließlich des Rechts auf den Schutz personenbezogener Daten, verletzt werden²³⁹. In diesem Zusammenhang kann ein Gericht beispielsweise anordnen, dass die Datenverantwortlichen eine rechtswidrige Tätigkeit aussetzen oder einstellen. Darüber hinaus können Datenschutzrechte, einschließlich der durch das LGPD geschützten Rechte, durch zivilrechtliche Klagen durchgesetzt werden. Gemäß Artikel 22 LGPD ist es ausdrücklich möglich, dass betroffene Personen ihre Rechte vor Gericht geltend machen können und natürliche Personen einzeln oder kollektiv Rechtssachen im Zusammenhang mit dem Datenschutz vor Gericht bringen können.
- (153) Das brasilianische System bietet daher verschiedene Möglichkeiten, einen Rechtsbehelf einzulegen, angefangen bei leicht zugänglichen, kostengünstigen Möglichkeiten (z. B. eine Beschwerde bei der ANPD) bis hin zu gerichtlichen Verfahren, in deren Rahmen auch die Möglichkeit besteht, Schadenersatzansprüche geltend zu machen oder kollektive Rechtsbehelfsverfahren einzulegen.
3. ZUGANG ZU UND VERWENDUNG VON AUS DER EUROPÄISCHEN UNION ÜBERMITTELTEN PERSONENBEZOGENEN DATEN DURCH BEHÖRDEN IN BRASILIAN
- (154) Die Kommission hat auch die Einschränkungen und Garantien geprüft, einschließlich der Aufsichtsmechanismen und Rechtsbehelfe für natürliche Personen, die nach brasilianischem Recht in Bezug auf die Erhebung und nachfolgende Verwendung personenbezogener Daten durch brasilianische Behörden, die im öffentlichen Interesse an Datenverantwortliche und Auftragsverarbeiter in Brasilien übermittelt wurden, insbesondere zur Strafverfolgung und zur nationalen Sicherheit (im Folgenden „staatlicher Zugriff“), verfügbar sind.
- (155) Bei der Beurteilung der Frage, ob die Bedingungen für den staatlichen Zugriff auf Daten, die gemäß diesem Beschluss an Brasilien übermittelt werden, das Kriterium der „wesentlichen Gleichwertigkeit“ nach Artikel 45 Absatz 1 der Verordnung (EU) 2016/679 in der Auslegung des Gerichtshofs der Europäischen Union im Lichte der Charta der Grundrechte erfüllen, hat die Kommission insbesondere die folgenden Kriterien berücksichtigt.
- (156) Erstens muss jede Einschränkung des Rechts auf den Schutz personenbezogener Daten gesetzlich vorgesehen sein, und die gesetzliche Grundlage für den Eingriff in dieses

²³⁸ Artikel 45 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

²³⁹ Das Oberste Bundesgericht Brasiliens erließ 2020 ein Urteil, mit dem eine Präsidialverordnung eingestellt wurde, die Telekommunikationsunternehmen dazu verpflichtet hätte, Teilnehmerdaten an die Volkszählungsbehörde weiterzugeben; damit erkannte es erstmals den Datenschutz als Grundrecht an und ebnete den Weg für die Aufnahme dieses Rechts in die brasilianische Verfassung. Siehe Oberstes Bundesgericht, Entscheidung in der Rechtssache ADI 6387 vom 7. Mai 2020. Abrufbar unter: <https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf>.

Recht muss ihrerseits den Umfang der Einschränkung der Ausübung des betreffenden Rechts festlegen.²⁴⁰

- (157) Zweitens: Um dem Erfordernis der Verhältnismäßigkeit zu genügen, wonach Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten nur insoweit gelten dürfen, als dies in einer demokratischen Gesellschaft zur Verwirklichung spezifischer Ziele von allgemeinem Interesse, die den von der Union anerkannten Zielen gleichwertig sind, unbedingt erforderlich ist, muss die Rechtsvorschrift des betreffenden Drittlands, nach der der Eingriff zulässig ist, klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindestanforderungen aufstellen, sodass die Personen, deren Daten übermittelt wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen²⁴¹. In der Rechtsvorschrift muss insbesondere angegeben sein, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf²⁴²; ferner muss die Erfüllung dieser Anforderungen einer unabhängigen Aufsicht unterliegen²⁴³.
- (158) Drittens müssen diese Rechtsvorschriften und ihre Anforderungen nach dem nationalen Recht rechtsverbindlich sein. Dies betrifft in erster Linie die Behörden des betreffenden Drittlandes, aber diese rechtlichen Anforderungen müssen auch vor Gericht gegen diese Behörden durchsetzbar sein²⁴⁴. Insbesondere müssen betroffene Personen die Möglichkeit haben, Rechtsbehelfe vor einem unabhängigen und unparteiischen Gericht einzulegen, um Zugang zu den sie betreffenden personenbezogenen Daten zu erlangen oder die Berichtigung oder Löschung solcher Daten zu erwirken²⁴⁵.

3.1. Allgemeiner Rechtsrahmen

- (159) Die Einschränkungen und Garantien für die Erhebung und anschließende Verwendung personenbezogener Daten durch brasilianische Behörden ergeben sich aus dem übergeordneten verfassungsrechtlichen Rahmen, den speziellen Gesetzen, in denen ihre Tätigkeiten in den Bereichen Strafverfolgung und nationale Sicherheit geregelt sind, sowie aus den Vorschriften, die speziell für die Verarbeitung personenbezogener Daten gelten.
- (160) Erstens unterliegt der Zugang brasilianischer Behörden zu personenbezogenen Daten dem in der brasilianischen Verfassung verankerten allgemeinen Grundsatz der

²⁴⁰ Schrems II, Rn. 174 und 175 und die darin aufgeführte Rechtsprechung. Zum Zugriff durch Behörden der Mitgliedstaaten siehe auch Rechtssache C-623/17, „Privacy International“, ECLI:EU:C:2020:790, Rn. 65 sowie die verbundenen Rechtssachen C-511/18, C-512/18 und C-520/18, „La Quadrature du Net u. a.“, ECLI:EU:C:2020:791, Rn. 175.

²⁴¹ Schrems II, Rn. 176 und 181 sowie die darin aufgeführte Rechtsprechung. Zum Zugriff durch Behörden der Mitgliedstaaten siehe auch die Rechtssache Privacy International, Rn. 68 und La Quadrature du Net u. a., Rn. 132.

²⁴² Schrems II, Rn. 176. Zum Zugriff durch Behörden der Mitgliedstaaten siehe auch die Rechtssachen Privacy International, Rn. 68 und La Quadrature du Net u. a., Rn. 132.

²⁴³ Schrems II, Rn. 179.

²⁴⁴ Schrems II Rn. 181 und 182.

²⁴⁵ Schrems I, Rn. 95 und Schrems II, Rn. 194. In diesem Zusammenhang hat der EuGH insbesondere betont, dass die Einhaltung von Artikel 47 der Charta der Grundrechte, der das Recht auf einen wirksamen Rechtsbehelf vor einem unabhängigen und unparteiischen Gericht garantiert, „für das in der Union erforderliche Schutzniveau maßgebend ist und [von der] Kommission [festgestellt werden] muss, bevor sie einen Angemessenheitsbeschluss im Sinne von Artikel 45 Absatz 1 der [Verordnung (EU) 2016/679] erlässt“ (Schrems II, Rn. 186).

Rechtmäßigkeit, aus dem sich die Grundsätze der Angemessenheit, der Notwendigkeit und der Verhältnismäßigkeit ableiten²⁴⁶. Insbesondere dürfen die Grundrechte und Grundfreiheiten (einschließlich des Rechts auf Privatsphäre und Datenschutz) nach Artikel 5 der Verfassung nur dann gesetzlich eingeschränkt werden, wenn dies aus Gründen der nationalen Sicherheit, der öffentlichen Sicherheit oder anderen gesetzlich festgelegten besonderen Gründen des öffentlichen Interesses erforderlich ist. Solche Beschränkungen müssen angemessen und verhältnismäßig sein²⁴⁷. Insbesondere ist die Beurteilung des im öffentlichen Interesse liegenden Zwecks für die Beurteilung der Verhältnismäßigkeit des Eingriffs im Lichte des Grundsatzes der Rechtmäßigkeit unerlässlich. In Artikel 5 Ziffer LIV der Verfassung heißt es weiter: „Niemand darf ohne ein ordentliches Verfahren seiner Freiheit oder seines Eigentums beraubt werden“.

- (161) Zweitens garantiert die brasilianische Anordnung *Habeas Data* als verfassungsrechtlichen Rechtsbehelf zum Schutz des Rechts auf Zugang zu sowie auf Berichtigung und Löschung von personenbezogenen Daten, die sich im Besitz von Behörden oder in öffentlichen Datensätzen oder Registern befinden²⁴⁸. Sie dient als Schutz vor Missbrauch oder Verletzung der Privatsphäre im Zusammenhang mit der Datenverarbeitung durch öffentliche Stellen. Jede natürliche Person kann unabhängig von ihrer Staatsangehörigkeit einen Antrag auf der Grundlage von *Habeas Data* stellen²⁴⁹.
- (162) Drittens spiegeln sich die in den Erwägungsgründen 155 bis 158 genannten allgemeinen Grundsätze und Rechte auch in den spezifischen Gesetzen wider, die die Befugnisse der Strafverfolgungsbehörden und der nationalen Sicherheitsbehörden regeln. So sieht das Zivilrechtliche Rahmenwerk für das Internet beispielsweise Maßnahmen vor, die eine vorherige richterliche Anordnung für den Zugang zu Daten und eine Beschränkung des Zugriffs auf Online-Daten vorschreiben²⁵⁰. Ebenso sieht das Gesetz über die telefonische Überwachung spezifische Maßnahmen und Garantien für die Verarbeitung von Telekommunikationsdaten vor²⁵¹. Im Bereich der nationalen Sicherheit sieht das Gesetz zur Einrichtung des brasilianischen Nachrichtendienstes Maßnahmen für den rechtmäßigen Zugriff auf Daten zu Zwecken der nationalen Sicherheit vor²⁵².
- (163) Viertens unterliegt die Verarbeitung personenbezogener Daten durch Behörden, auch zu Zwecken der Strafverfolgung und der nationalen Sicherheit, den Datenschutzanforderungen des LGPD. Wie in Erwägungsgrund 31 dieses Beschlusses dargelegt, ist die im LGPD festgelegte Ausnahme für die Anwendung des LGPD im Bereich der öffentlichen Sicherheit, der Landesverteidigung, der Staatssicherheit

²⁴⁶ Artikel 5 Ziffer II der Verfassung der Föderativen Republik Brasilien von 1988.

²⁴⁷ Brasilien unterliegt der Zuständigkeit des Interamerikanischen Gerichtshofs für Menschenrechte, der unter anderem den Grundsatz der Verhältnismäßigkeit als „in einer demokratischen Gesellschaft wesentlich“ anerkannt hat und festgestellt hat, dass Einschränkungen der Grundrechte nur zulässig sind, wenn sie einem zwingenden öffentlichen Zweck dienen. Siehe z. B. MENDES, Gilmar Ferreira. Fundamental rights and judicial control [Grundrechte und gerichtliche Kontrolle]. São Paulo: Saraiva, 2012, S. 78.

²⁴⁸ Artikel 5 Ziffern LXXII und LXXVII der Verfassung der Föderativen Republik Brasilien 1988.

²⁴⁹ Siehe auch Erwägungsgründe 9 und 11 dieses Beschlusses.

²⁵⁰ Gesetz Nr. 12.965 vom 23. April 2014, Marco Civil da Internet („Zivilrechtliches Rahmenwerk für das Internet“). Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm.

²⁵¹ Gesetz Nr. 9.296 vom 24. Juli 1996 über die telefonische Überwachung. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/leis/19296.htm.

²⁵² Gesetz Nr. 9.883 vom 7. Dezember 1999. Gesetz zur Einrichtung des brasilianischen Nachrichtendienstes.

sowie der Untersuchung und Verfolgung von Straftaten nur teilweise gegeben. Das Oberste Bundesgericht hat die Anwendbarkeit des LGPD im Lichte des verfassungsmäßigen Schutzes personenbezogener Daten ausgelegt und festgestellt, dass die wichtigsten Grundsätze, Rechte und Ziele des LGPD für jede Verarbeitung personenbezogener Daten durch Behörden gelten, auch wenn sie für die Zwecke der Strafverfolgung oder der nationalen Sicherheit erfolgt²⁵³. Auf dieser Grundlage hat die ANPD beispielsweise Untersuchungen durchgeführt und Leitlinien herausgegeben, wie einen technischen Vermerk für Behörden für Tätigkeiten im Zusammenhang mit der öffentlichen Sicherheit, in denen sie darauf hinweist, dass die Verarbeitung für diese Zwecke des öffentlichen Interesses mit den allgemeinen Grundsätzen und Rechten des LGPD im Einklang stehen muss²⁵⁴.

- (164) Schließlich kann sich der Einzelne vor dem Obersten Bundesgericht auf seine Grundrechte und -freiheiten berufen, wenn er glaubt, dass sie von Behörden bei der Ausübung ihrer Befugnisse verletzt worden sind. Wie in den Erwägungsgründen 143 bis 153 dieses Beschlusses dargelegt, können natürliche Personen auch bei unabhängigen Aufsichtsgremien (z. B. der ANPD) und Gerichten Rechtsbehelfe in Bezug auf ihre Datenschutzrechte einlegen.

3.2. Zugriff und Verwendung durch brasilianische Behörden für Strafverfolgungszwecke

- (165) In den Rechtsvorschriften Brasiliens sind neben einer Reihe von Einschränkungen für den Zugang zu und die Verwendung von personenbezogenen Daten für die Zwecke der Strafverfolgung Aufsichtsmechanismen und Rechtsbehelfe vorgesehen, die den in den Erwägungsgründen 155 bis 158 dieses Beschlusses genannten Anforderungen entsprechen. Die folgenden Abschnitte enthalten eine detaillierte Prüfung der Bedingungen, unter denen ein solcher Zugriff erfolgen kann, sowie der Garantien, die für die Nutzung dieser Befugnisse gelten.

3.2.1. Rechtsgrundlage, Einschränkungen und Garantien

- (166) In der Regel erfolgt der Zugriff auf personenbezogene Daten durch Behörden zu Strafverfolgungszwecken auf der Grundlage einer vorherigen richterlichen Anordnung einer zuständigen Justizbehörde²⁵⁵. Abweichend von dieser Regel haben Polizei- und Strafverfolgungsbehörden in Fällen, die im Gesetz ausdrücklich vorgesehen sind, Zugang zu den Daten von Personen, gegen die ermittelt wird und die in einem öffentlichen Register erfasst sind, d. h. zu Daten über die persönliche Qualifikation, Zugehörigkeit und Anschrift²⁵⁶. Die im Gesetz vorgesehene erschöpfende Liste der zugänglichen Register umfasst Informationen über Brasilianer oder Personen mit Wohnsitz in Brasilien und würde nicht für den Zugang zu Daten gelten, die aus der EU übermittelt wurden und somit nicht in den Anwendungsbereich dieses Beschlusses fallen²⁵⁷. Der Zugang zu diesen Registern unterliegt dem Verfassungsgrundsatz der

²⁵³ Oberstes Bundesgericht. Entscheidung in der Rechtssache ADI 6649, September 2022. Abrufbar unter: <https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false>.

²⁵⁴ Technischer Vermerk Nr. 175/2023, Absatz 5.1.

²⁵⁵ Siehe beispielsweise Artikel 5 Ziffer XII der Verfassung der Föderativen Republik Brasilien von 1988.

²⁵⁶ Artikel 15 und 16 des Gesetzes Nr. 12.850 vom 2. August 2013 über kriminelle Vereinigungen und strafrechtliche Ermittlungen. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/112850.htm.

²⁵⁷ Zu den zugänglichen Registern gehören: Beschäftigungsregister, Wählerverzeichnisse, Telefonregister, Finanzregister, Register von Internetanbietern, Kreditkartenregister. Die Informationen in diesen Registern umfassen Informationen über Personen, die diese Dienste abonniert haben oder diese öffentlichen Dienste nutzen. Artikel 15 und 16 des Gesetzes Nr. 12.850 vom 2. August 2013 über kriminelle Vereinigungen und strafrechtliche Ermittlungen. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/112850.htm.

Rechtmäßigkeit – von dem sich die Grundsätze der Angemessenheit, Notwendigkeit und Verhältnismäßigkeit ableiten – und kann einer nachträglichen gerichtlichen Überprüfung unterzogen werden, wie in den Erwägungsgründen 159 bis 161 erläutert.

- (167) Die brasilianischen Behörden, die berechtigt sind, im Wege einer vorherigen richterlichen Anordnung auf personenbezogene Daten für strafrechtliche Zwecke zuzugreifen und diese zu erheben, sind 1) die Zivilpolizei, 2) die Bundespolizei, 3) die Staatsanwaltschaft des Bundesstaates, 4) die Bundesstaatsanwaltschaft, 5) Richter und Gerichte und 6) parlamentarische Untersuchungsausschüsse.
- (168) Nach Artikel 3-B des Strafgesetzbuchs kann ein Richter, der „für die Überwachung der Rechtmäßigkeit strafrechtlicher Ermittlungen und den Schutz der individuellen Rechte zuständig ist“, eine richterliche Anordnung erlassen, mit der Folgendes genehmigt wird: 1) telefonische Überwachung von Nachrichten über Computer und vernetzte Systeme oder andere Formen der Kommunikation, 2) die Aufhebung des Steuer-, Bank-, Daten- und Telefongeheimnisses, (3) Hausdurchsuchungen und Beschlagnahmen und 4) Zugang zu geheimen Informationen sowie 5) „andere Maßnahmen zur Erlangung von Beweismitteln, die die Grundrechte der von der Untersuchung betroffenen Person einschränken“²⁵⁸.

3.2.1.1. Abhörung des Fernmeldeverkehrs

- (169) Die Vertraulichkeit der elektronischen und telefonischen Kommunikation wird im brasilianischen Rechtsrahmen als Grundrecht betrachtet²⁵⁹.
- (170) Behörden können nur in Ausnahmefällen zum Zwecke strafrechtlicher Ermittlungen oder der Strafverfolgung auf diese Daten zugreifen. Wie vom Obersten Bundesgericht festgestellt, muss die Überwachung der Kommunikation stets eine subsidiäre und außergewöhnliche Maßnahme sein, die nur dann zulässig ist, wenn es keine anderen Möglichkeiten gibt, einen bestimmten Fall zu lösen²⁶⁰. Die Modalitäten für die Überwachung der Online- und Telefonkommunikation sind im Gesetz über die telefonische Überwachung geregelt²⁶¹.
- (171) Artikel 2 des Gesetzes über die telefonische Überwachung legt strenge Bedingungen für den Zugriff auf die Kommunikation fest. Jede Überwachung der Kommunikation bedarf einer vorherigen richterlichen Genehmigung. Ein gültiger Antrag auf Überwachung muss einem Richter von den ermächtigten Behörden vorgelegt werden, bei denen es sich entweder um 1) die zuständige Polizeibehörde im Rahmen einer strafrechtlichen Ermittlung oder 2) einen Vertreter der Staatsanwaltschaft im Rahmen einer strafrechtlichen Ermittlung und Strafverfolgung handeln kann²⁶². Die Überwachung von Telefongesprächen ist unter folgenden Umständen, die den Anforderungen der Notwendigkeit und Verhältnismäßigkeit entsprechen, nicht zulässig: 1) wenn keine hinreichenden Beweise für die Täterschaft oder die Beteiligung an einer Straftat vorliegen, 2) wenn die Beweise mit anderen verfügbaren Mitteln erbracht werden können, 3) wenn der ermittelte Sachverhalt eine Straftat darstellt, die mit Freiheitsentzug geahndet werden kann²⁶³.

²⁵⁸ Gesetzesdekret Nr. 3.689 vom 3. Oktober 1941, Strafgesetzbuch. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

²⁵⁹ Artikel 5 Ziffer XII der Verfassung der Föderativen Republik Brasilien von 1988.

²⁶⁰ Oberstes Bundesgericht in der Rechtssache HC 108147/PR, 2012. Abrufbar unter: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401>.

²⁶¹ Artikel 1 des Gesetzes Nr. 9.296 vom 24. Juli 1996 über die telefonische Überwachung.

²⁶² Artikel 2 Ziffern I und II des Gesetzes Nr. 9.296 vom 24. Juli 1996 über die telefonische Überwachung.

²⁶³ Artikel 2 des Gesetzes Nr. 9.296 vom 24. Juli 1996 über die telefonische Überwachung.

- (172) Darüber hinaus schreibt das Gesetz über die telefonische Überwachung vor, dass in dem Antrag auf Überwachung die Notwendigkeit der Maßnahme darzulegen ist²⁶⁴. Die vorherige richterliche Genehmigung muss begründet sein, und die Verhältnismäßigkeit der zur Durchführung der Überwachung eingesetzten Mittel ist zu berücksichtigen²⁶⁵. Der Richter kann den Zugriff auf den Inhalt der Kommunikation für höchstens 15 Tage genehmigen. Dieser Zeitraum kann durch eine neue richterliche Entscheidung verlängert werden, sofern die Unerlässlichkeit der Maßnahme nachgewiesen wird²⁶⁶. Jede Überwachung von Kommunikation, einschließlich Umgebungsüberwachung, die ohne richterliche Genehmigung oder zu gesetzlich nicht zulässigen Zwecken erfolgt, stellt eine Straftat dar, die mit bis zu vier Jahren Freiheitsentzug geahndet werden kann²⁶⁷.
- (173) In der Regel werden Daten, auf die gemäß dem Gesetz über die telefonische Überwachung zu strafrechtlichen Zwecken zugegriffen werden kann und die zu diesen Zwecken erhoben werden dürfen, gemäß den verbindlichen Leitlinien der Justiz für die Dauer der Verarbeitung aufbewahrt und anschließend gelöscht, sobald sie nicht mehr für ein Gerichtsverfahren benötigt werden²⁶⁸. In Artikel 9 des Gesetzes über die telefonische Überwachung ist ferner festgelegt, dass die Daten „unbrauchbar“ zu machen sind, wenn die erhobenen Inhalte nicht mit dem in der Rechtssache untersuchten Sachverhalt in Zusammenhang stehen²⁶⁹.
- (174) In Bezug auf Telekommunikations-Metadaten sind Telefonunternehmen gemäß Artikel 17 des Gesetzes über kriminelle Organisationen und strafrechtliche Ermittlungen verpflichtet, Informationen über Nutzerkonten von Personen mit Wohnsitz in Brasilien und Aufzeichnungen von Telefongesprächen (ausschließlich Telefonnummern) fünf Jahre lang aufzubewahren²⁷⁰. Der Zugang zu diesem von ANATEL (der brasilianischen Regulierungsagentur für Telekommunikation) geführten Register ist auf bestimmte öffentliche Einrichtungen beschränkt und erfordert, wie oben beschrieben, eine richterliche Genehmigung.
- (175) In Bezug auf online verfügbare Informationen garantiert Artikel 7 des Zivilrechtlichen Rahmenwerks für das Internet „die Unverletzlichkeit und Vertraulichkeit der Kommunikation über das Internet“, mit Ausnahme einer richterlichen Anordnung gemäß den gesetzlichen Bestimmungen; sowie „die Unverletzlichkeit und Vertraulichkeit gespeicherter privater Kommunikation, mit Ausnahme einer richterlichen Anordnung“²⁷¹.
- (176) Nach Artikel 10 des Zivilrechtlichen Rahmenwerks für das Internet kann der Zugriff auf den Inhalt der Online-Kommunikation und auf Verbindungsdaten (einschließlich Metadaten) nur durch vorherige richterliche Anordnung erfolgen. Nach Artikel 22 des Zivilrechtlichen Rahmenwerks für das Internet muss der Antrag auf Erlass einer richterlichen Anordnung Folgendes enthalten: Ziffer i) stichhaltige Beweise für das

²⁶⁴ Artikel 4 des Gesetzes Nr. 9.296 vom 24. Juli 1996 über die telefonische Überwachung.

²⁶⁵ Artikel 5 des Gesetzes Nr. 9.296 vom 24. Juli 1996 über die telefonische Überwachung.

²⁶⁶ Artikel 5 des Gesetzes Nr. 9.296 vom 24. Juli 1996 über die telefonische Überwachung.

²⁶⁷ Artikel 10 des Gesetzes Nr. 9.296 vom 24. Juli 1996 über die telefonische Überwachung.

²⁶⁸ Artikel 20 der Entschließung Nr. 324 vom 20. Juni 2020. Abrufbar unter: <https://www.gov.br/conarq/pt-br/legislacao-arquivistica/atos-do-poder-judiciario/resolucao-no-324-de-30-de-junho-de-2020>.

²⁶⁹ Artikel 9 des Gesetzes Nr. 9.296 vom 24. Juli 1996 über die telefonische Überwachung.

²⁷⁰ Artikel 17 des Gesetzes Nr. 12.850 vom 2. August 2013 über kriminelle Vereinigungen und strafrechtliche Ermittlungen. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/12850.htm.

²⁷¹ Artikel 7 des Gesetzes Nr. 12.965 vom 23. April 2014, Marco Civil da Internet („Zivilrechtliches Rahmenwerk für das Internet“).

Vorliegen der Straftat, Ziffer ii) eine Begründung des Nutzens der angeforderten Aufzeichnungen für Ermittlungs- oder Beweis Zwecke und Ziffer iii) den Zeitraum, auf den sich die Aufzeichnungen beziehen. Artikel 13 schreibt ferner vor, dass Internet- oder Anwendungsdienstleister Verbindungsprotokolle für ein Jahr „in einer kontrollierten und gesicherten Umgebung“ aufbewahren müssen²⁷². Eine ähnliche Verpflichtung zur Aufbewahrung von Daten in Bezug auf den Inhalt der Online-Kommunikation besteht nicht. Zugang zu den gespeicherten Aufzeichnungen der Verbindungsprotokolle kann einer zuständigen Behörde nur auf der Grundlage einer richterlichen Genehmigung unter den in diesem Erwägungsgrund beschriebenen Bedingungen gewährt werden²⁷³.

- (177) In Artikel 11 des Zivilrechtlichen Rahmenwerks für das Internet wird darauf hingewiesen, dass bei allen Vorgängen, die die Erhebung, Speicherung, Aufbewahrung oder sonstige Verarbeitung von Protokollen, personenbezogenen Daten oder Kommunikation durch Anbieter von Verbindungen und Internetanwendungen in Brasilien umfassen, „die brasilianischen Rechtsvorschriften und die Rechte auf Privatsphäre, den Schutz personenbezogener Daten und die Vertraulichkeit privater Kommunikation und privater Aufzeichnungen“ zu beachten sind. Aus den in den Erwägungsgründen 175 bis 177 dargelegten Garantien ergibt sich, dass die massenhafte Erhebung und Vorratsspeicherung von Internetkommunikationsdaten in Brasilien im Allgemeinen nicht zulässig ist.

3.2.1.2. Aufhebung des Schutzes von Steuer-, Bank-, Daten- und Kommunikationsgeheimnissen

- (178) In Brasilien besteht ein verfassungsrechtlicher Schutz für die Vertraulichkeit der elektronischen und telefonischen Kommunikation (einschließlich der Datenkommunikation)²⁷⁴. Das LGPD schützt ferner die Nutzung von Daten und Kommunikationsinformationen²⁷⁵, während das Gesetz über die Vertraulichkeit von Finanzinstituten die Vertraulichkeit von Steuer- und Bankinformationen schützt²⁷⁶.
- (179) Behörden können diese Informationen nur in Ausnahmefällen zum Zwecke der strafrechtlichen Ermittlungen oder der Strafverfolgung einsehen. Wie vom Obersten Bundesgericht festgestellt, muss die Überwachung der Kommunikation stets eine subsidiäre und außergewöhnliche Maßnahme sein, die nur dann zulässig ist, wenn es keine anderen Möglichkeiten gibt, einen bestimmten Fall zu lösen²⁷⁷.
- (180) Die Kriterien und Garantien für den Zugang zu Daten und Kommunikation sind im Zivilrechtlichen Rahmenwerk für das Internet und im Gesetz über telefonische Überwachung festgelegt und werden in den Erwägungsgründen 169 bis 177 dieses Beschlusses näher ausgeführt.
- (181) In Bezug auf Steuer- und Bankdaten sind in Artikel 1 des Gesetzes über die Vertraulichkeit von Finanzinstituten die Bedingungen für die Aufhebung der

²⁷² Artikel 13 Hauptsatz des Gesetzes Nr. 12.965 vom 23. April 2014, Marco Civil da Internet („Zivilrechtliches Rahmenwerk für das Internet“).

²⁷³ Artikel 13 Absatz 5 des Gesetzes Nr. 12.965 vom 23. April 2014, Marco Civil da Internet („Zivilrechtliches Rahmenwerk für das Internet“).

²⁷⁴ Artikel 5 Ziffer XII der Verfassung der Föderativen Republik Brasilien von 1988.

²⁷⁵ Siehe Artikel 2 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

²⁷⁶ Ergänzendes Gesetz Nr. 105 vom 10. Januar 2001 über die Vertraulichkeit von Finanzinstituten. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

²⁷⁷ Oberstes Bundesgericht in der Rechtssache HC 108147/PR, 2012. Abrufbar unter: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401>.

allgemeinen Verpflichtung zur Gewährleistung der Vertraulichkeit dieser Informationen festgelegt. Erstens kann die Vertraulichkeit nur durch eine richterliche Genehmigung aufgehoben werden²⁷⁸. Zweitens können die Maßnahmen nur für strafrechtliche Ermittlungen oder die Verfolgung bestimmter Straftaten oder Verbrechen genehmigt werden, nämlich 1) Terrorismus, 2) unerlaubter Handel mit Suchtstoffen oder ähnlichen Drogen, 3) Schmuggel von Waffen, Munition oder Material, das zu ihrer Herstellung bestimmt ist, oder Handel damit, 4) Erpressung durch Entführung, 5) Straftaten gegen das nationale Finanzsystem, 6) Straftaten gegen die öffentliche Verwaltung, 7) Straftaten gegen das Steuersystem und die soziale Sicherheit, 8) Geldwäsche oder Verschleierung von Vermögenswerten und 9) Verbindung zu einer kriminellen Vereinigung²⁷⁹. In Artikel 10 des Gesetzes ist ferner festgelegt, dass der Schutz der Vertraulichkeit von Steuer- und Bankdaten nicht für andere Zwecke aufgehoben werden darf und dass die Nichteinhaltung dieser Beschränkung eine Straftat darstellt, die mit einer Freiheitsstrafe von bis zu vier Jahren geahndet werden kann²⁸⁰.

3.2.1.3. Durchsuchung und Beschlagnahme

- (182) Die Bundesverfassung sieht in der Regel vor, dass Durchsuchungen und Beschlagnahmen nur unter genau festgelegten außergewöhnlichen Umständen oder nach Maßgabe der gesetzlichen Bestimmungen und auf der Grundlage einer richterlichen Anordnung einer zuständigen Justizbehörde und unter Wahrung eines ordnungsgemäßen Verfahrens durchgeführt werden dürfen²⁸¹. Durchsuchungen und Beschlagnahmen müssen dem Grundsatz der Rechtmäßigkeit entsprechen und dürfen nur im erforderlichen Umfang durchgeführt werden.
- (183) In folgenden Ausnahmefällen können Durchsuchungen und Beschlagnahmen ohne richterliche Anordnung erfolgen: 1) im Fall einer auf frischer Tat festgestellten Straftat (d. h. wenn eine Straftat in Anwesenheit von Strafverfolgungsbehörden begangen wird), 2) im Falle einer Naturkatastrophe (um Menschenleben oder Eigentum zu retten) oder 3) um einer Person, die nicht in der Lage ist, ihre Einwilligung zu erteilen, Hilfe zu leisten²⁸². In der Rechtsprechung des brasilianischen Obersten Bundesgerichts wurde klargestellt, dass Strafverfolgungsbehörden sich nicht auf „anonyme Hinweise“ und „verdächtiges Verhalten“ stützen dürfen, um Durchsuchungen oder Beschlagnahmen ohne Anordnung durchzuführen, da dies nicht den Anforderungen der Rechtmäßigkeit entspricht und den Behörden keine stichhaltige Begründung für die Verletzung der Unverletzlichkeit der Wohnung liefert²⁸³.
- (184) Hinsichtlich der Verfahrensgarantien darf gemäß den brasilianischen Verfassungsgrundsätzen keine Durchsuchung elektronischer Geräte erfolgen, ohne dass ein begründeter Verdacht besteht, dass auf dem Gerät strafbare Handlungen gespeichert sind, und in der Regel auch nicht ohne richterliche Anordnung²⁸⁴. Darüber hinaus kann eine natürliche Person nicht zur Herausgabe von Daten gezwungen

²⁷⁸ Artikel 3-B, Gesetzesdekret Nr. 3.689 vom 3. Oktober 1941, Strafgesetzbuch. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

²⁷⁹ Artikel 1 Absatz 4 Ziffern I bis IX des ergänzenden Gesetzes Nr. 105 vom 10. Januar 2001 über die Vertraulichkeit von Finanzinstituten. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

²⁸⁰ Artikel 10 des ergänzenden Gesetzes Nr. 105 vom 10. Januar 2001 über die Vertraulichkeit von Finanzinstituten. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

²⁸¹ Artikel 5 Ziffer XI der Verfassung der Föderativen Republik Brasilien von 1988.

²⁸² Artikel 5 Ziffer XI der Verfassung der Föderativen Republik Brasilien von 1988.

²⁸³ Oberstes Bundesgericht, 2020, in der Rechtssache J. S., Außerordentlicher Rechtsbehelf Nr. 603616.

²⁸⁴ Artikel 5 Ziffer XI der Verfassung der Föderativen Republik Brasilien von 1988.

werden, wenn diese Herausgabe ihre verfassungsmäßigen Rechte, wie beispielsweise das Recht, sich nicht selbst belasten zu müssen, verletzen würde²⁸⁵. Bei der Einreichung eines Antrags auf Erlass eines Durchsuchungsbeschlusses bei Gericht muss die Strafverfolgungsbehörde die einschlägigen Tatsachen und Beweise vorlegen, die die Notwendigkeit des Zugriffs auf das Computersystem und die Daten unter Verwendung rechtmäßig erlangter Zugangsdaten belegen²⁸⁶. Erlässt das Gericht den Durchsuchungsbeschluss, so verwenden die Behörden die Zugangsdaten, um gemäß den im Beschluss festgelegten Bedingungen auf das Computersystem und die darin enthaltenen Daten zuzugreifen. Nach Abschluss der Durchsuchung oder des Zugriffs müssen die zuständigen Behörden dem Gericht einen Bericht vorlegen, in dem die Ergebnisse der Durchsuchung oder des Zugriffs beschrieben und eine Liste der erhaltenen Daten oder Informationen vorgelegt werden.

3.2.1.4. Zugang zu vertraulichen Informationen

- (185) Artikel 4 des Gesetzes über den Zugang zu Informationen definiert „vertrauliche Informationen“ als Informationen, die „aufgrund ihrer wesentlichen Bedeutung für die Sicherheit der Gesellschaft und des Staates vorübergehend einer Beschränkung des öffentlichen Zugangs unterliegen“²⁸⁷. Personenbezogene Daten können zum Geltungsbereich vertraulicher Informationen im Sinne des vorstehenden Satzes gehören.
- (186) Nach Artikel 6 des Gesetzes über den Zugang zu Informationen sind öffentliche Stellen verpflichtet, vertrauliche Informationen zu schützen und den Zugang zu ihnen zu beschränken. Wie vom Obersten Bundesgericht und durch die gesetzlichen Bestimmungen festgelegt, kann im Hinblick auf den Zugang zu Kommunikations-, Daten-, Bank- und Steuerinformationen der Zugang zu vertraulichen Informationen für strafrechtliche Ermittlungen und Strafverfolgungsmaßnahmen nur in Ausnahmefällen auf der Grundlage einer richterlichen Genehmigung erfolgen und ist nur zulässig, wenn es keine anderen Möglichkeiten gibt, einen bestimmten Fall zu lösen²⁸⁸.

3.2.1.5. Andere Maßnahmen zur Erlangung von Beweismitteln, die die Grundrechte der von der Untersuchung betroffenen Person einschränken

- (187) „Andere Maßnahmen zur Erlangung von Beweismitteln, die die Grundrechte der von der Untersuchung betroffenen Person einschränken“ beziehen sich beispielsweise auf die Möglichkeit, eine Untersuchungshaft anzuordnen oder eine Person unter physische Überwachung zu stellen. Diese Maßnahmen sind im Zusammenhang mit der Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses grundsätzlich nicht von Bedeutung.
- (188) Der Vollständigkeit halber sei angemerkt, dass solche von einer Behörde vorgeschlagenen Maßnahmen nur auf der Grundlage einer richterlichen Genehmigung durchgeführt werden dürfen. Wie vom Obersten Bundesgericht festgelegt, müssen die vorgeschlagenen Maßnahmen mit dem in der Verfassung verankerten Grundsatz der

²⁸⁵ Artikel 5 Ziffer LXIII der Verfassung der Föderativen Republik Brasilien von 1988. Siehe auch Gesetzesdekret Nr. 2.848 vom 7. Dezember 1940, Strafprozessordnung. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

²⁸⁶ Artikel 240, Gesetzesdekret Nr. 2.848 vom 7. Dezember 1940, Strafprozessordnung.

²⁸⁷ Artikel 4 Ziffer III des Gesetzes Nr. 12.527 vom 18. November 2011 über den Zugang zu Informationen.

²⁸⁸ Oberstes Bundesgericht in der Rechtssache HC 108147/PR, 2012. Abrufbar unter: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401> und Artikel 3-B, Gesetzesdekret Nr. 3.689 vom 3. Oktober 1941, Strafgesetzbuch. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

Rechtmäßigkeit im Einklang stehen und können nur in Ausnahmefällen und wenn es keine Alternative gibt, angeordnet werden.

3.2.2. Weitere Verwendung der Daten

- (189) Hinsichtlich der weiteren Verwendung personenbezogener Daten für einen anderen Zweck durch eine Behörde sieht Artikel 9 des Gesetzes über die telefonische Überwachung vor, dass die Daten „unbrauchbar“ zu machen sind, wenn die erhobenen Inhalte nicht mit dem in einer bestimmten Rechtssache untersuchten Sachverhalt in Zusammenhang stehen. Artikel 13 des Zivilrechtlichen Rahmenwerks für das Internet beschränkt zudem die Speicherung von Verbindungsdaten in einem Register auf höchstens ein Jahr. Artikel 10 des Gesetzes über die Vertraulichkeit von Finanzinstituten schränkt auch den Zweck ein, zu dem die Vertraulichkeit von Steuer- und Bankdaten aufgehoben werden darf²⁸⁹. Diese Maßnahmen beschränken in der Praxis die Möglichkeit einer weiteren Verwendung der Daten.
- (190) Darüber hinaus und vor allem hat das Oberste Bundesgericht entschieden, dass das LGPD für die Weitergabe personenbezogener Daten zwischen öffentlichen Stellen gilt, auch wenn es sich um eine Weitergabe zwischen Strafverfolgungsbehörden und Nachrichtendiensten handelt²⁹⁰. Das Oberste Bundesgericht wies insbesondere darauf hin, dass „die Weitergabe personenbezogener Daten zwischen öffentlichen Verwaltungsstellen und Einrichtungen Folgendes voraussetzt: 1) die Definition eines berechtigten, spezifischen und eindeutigen Zwecks der Datenverarbeitung, 2) die Vereinbarkeit der Verarbeitung mit den angegebenen Zwecken, 3) die Beschränkung der Weitergabe auf das zur Erreichung des angegebenen Zwecks erforderliche Mindestmaß sowie die uneingeschränkte Einhaltung der im LGPD festgelegten Anforderungen, Garantien und Verfahren, soweit sie mit dem öffentlichen Sektor vereinbar sind.“ Das Oberste Bundesgericht fügte hinzu, dass gemäß Artikel 42 LGPD „die Verarbeitung personenbezogener Daten durch öffentliche Stellen, die gegen die gesetzlichen und verfassungsrechtlichen Vorgaben verstößt, die zivilrechtliche Haftung des Staates für Schäden auslöst, die der Person entstanden sind“.
- (191) Hinsichtlich der Weitergabe personenbezogener Daten zwischen Strafverfolgungsbehörden in Brasilien und ähnlichen Behörden in Drittländern unterliegen diese Tätigkeiten im Einklang mit dem LGPD den völkerrechtlichen Instrumenten. In diesem Zusammenhang sieht Artikel 33 Ziffer III LGPD vor, dass internationale Datenübermittlungen zulässig sind, wenn „dies für die internationale rechtliche Zusammenarbeit zwischen öffentlichen Stellen der Nachrichtendienste, Untersuchungs- und Strafverfolgungsbehörden im Einklang mit internationalen Rechtsinstrumenten erforderlich ist“. In Brasilien fungiert das Ministerium für Justiz und öffentliche Sicherheit als zentrale Behörde für die internationale justizielle Zusammenarbeit in Strafsachen. Das Ministerium ist für die Entgegennahme, Analyse, Übermittlung und Überwachung der Bearbeitung von Ersuchen um internationale Zusammenarbeit mit ausländischen Behörden unter Einhaltung der geltenden völkerrechtlichen Vorschriften und des LGPD zuständig. Die für die internationale rechtliche Zusammenarbeit erforderliche Verarbeitung personenbezogener Daten unterliegt den Grundsätzen der Zweckbindung (Artikel 6 Ziffer I LGPD), der Rechtmäßigkeit der Verarbeitung und Verarbeitung nach Treu und Glauben (Artikel 6

²⁸⁹ Artikel 10 des ergänzenden Gesetzes Nr. 105 vom 10. Januar 2001 über die Vertraulichkeit von Finanzinstituten. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

²⁹⁰ Oberstes Bundesgericht. Entscheidung in der Rechtssache ADI 6649, September 2022. Abrufbar unter: <https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false>.

und 7 LGPD), der Datenminimierung und Richtigkeit (Artikel 6 Ziffern III und V LGPD), der Transparenz (Artikel 6 Ziffer VI LGPD), der Datensicherheit (Artikel 6 Ziffer VII LGPD) und der Begrenzung der Speicherdauer (Artikel 6 Ziffern I, III, IV und Artikel 16 LGPD). Eine etwaige Weitergabe personenbezogener Daten an Dritte (einschließlich Drittländer) kann nur im Einklang mit diesen Grundsätzen erfolgen, nachdem die Einhaltung der Verfassungsgrundsätze der Notwendigkeit und der Verhältnismäßigkeit geprüft und die Kontinuität des Schutzes und die Einhaltung der Rechte der betroffenen Personen sichergestellt wurden (Artikel 2 der Datenübermittlungsverordnung).

- (192) Die Befugnisse der Strafverfolgungsbehörden Brasiliens zur Erhebung von Daten und zum Zugriff auf Daten sind daher durch klare und präzise gesetzliche Vorschriften begrenzt und unterliegen einer Reihe von Garantien. Diese Garantien umfassen insbesondere eine garantierte Überwachung der Durchführung solcher Maßnahmen, unter anderem durch vorherige richterliche Genehmigung und Schutzmaßnahmen zur Begrenzung der Dauer des Zugriffs und der Speicherung der Informationen im Einklang mit den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit.

3.2.3. Aufsicht

- (193) Die Tätigkeit der Strafverfolgungsbehörden wird in Brasilien von verschiedenen Stellen beaufsichtigt.
- (194) Erstens ist die ANPD, wie das Oberste Bundesgericht bestätigt hat, befugt, die Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden unter bestimmten Voraussetzungen gemäß LGPD zu überwachen²⁹¹. In diesem Zusammenhang kann die ANPD ihre Untersuchungs- und Abhilfebefugnisse gemäß LGPD ausüben. So hat die ANPD beispielsweise die Tätigkeiten der Bundespolizei, des Ministeriums für Justiz und öffentliche Sicherheit und anderer öffentlicher Stellen untersucht, die auf Ebene des Bundes, der Länder oder der Kommunen Sicherheitsaufgaben wahrnehmen oder für die Strafverfolgung zuständig sind²⁹². Untersuchungen können auf eigene Initiative der ANPD oder auf der Grundlage von Ersuchen und Beschwerden durchgeführt werden, die beispielsweise von natürlichen Personen, Organisationen der Zivilgesellschaft und Behörden eingereicht werden können. Die ANPD führte beispielsweise auf Ersuchen der Zivilgesellschaft mehrere Untersuchungen zum Einsatz von Videokameras durch²⁹³.
- (195) Zweitens wird die Tätigkeit der Strafverfolgungsbehörden in Brasilien von der Justiz beaufsichtigt. Die Gerichte sind unter den in den Erwägungsgründen 165 bis 187 genannten Umständen befugt, die Erhebung personenbezogener Daten und den Zugang dazu zu genehmigen. Sie sind ferner befugt, bei Missbrauch oder Nichteinhaltung der geltenden Rechtsvorschriften zivil- und strafrechtliche Sanktionen zu verhängen, wozu auch der Freiheitsentzug oder die Anordnung, bestimmte Tätigkeiten einzustellen, gehören.

²⁹¹ Siehe Erwägungsgrund 163 dieses Beschlusses und Oberstes Bundesgericht, Entscheidung in der Rechtssache ADI 6649 vom 15. September 2022. Abrufbar unter: <https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false>.

²⁹² Siehe ANPD, Überprüfungen, einschließlich der Verfahren 00261.000836/2021-76 und 00261.001028/2021-26. Abrufbar unter: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos?_authenticator=b05dbbec15247ce4c8b7065d588ef945f6d4d340.

²⁹³ Siehe ANPD, Überprüfungen, Verfahren 00261.002211/2022-20 betreffend den Einsatz von Überwachungskameras durch Behörden in der Stadt Fortaleza. Ersuchen an die ANPD, abrufbar unter: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos/arquivos-processos-de-fiscalizacao-concluidos/processossec_pblico00261-002211_2022-20.pdf.

- (196) Drittens ist die Staatsanwaltschaft, eine unabhängige und ständige Institution in Brasilien, die für die Verteidigung der Rechtsordnung und des demokratischen Systems zuständig ist, befugt, eine externe Kontrolle über polizeiliche Tätigkeiten auszuüben²⁹⁴. Wie im Beschluss über die Staatsanwaltschaft dargelegt, besteht der Zweck der externen Kontrolle der polizeilichen Tätigkeiten darin, die „Ordnungsmäßigkeit und Angemessenheit der bei der Ausübung polizeilicher Tätigkeiten angewandten Verfahren“ insbesondere im Hinblick auf die „Achtung der durch die Bundesverfassung und die Gesetze garantierten Grundrechte“ aufrechtzuerhalten²⁹⁵. In dieser Eigenschaft kann die Staatsanwaltschaft unter anderem jederzeit oder planmäßig Vor-Ort-Besuche durchführen, Ermittlungen überprüfen, die Beschlagnahme von Gütern beaufsichtigen und die Einhaltung von Haftbefehlen überwachen²⁹⁶. Jeder Verstoß gegen das Gesetz ist dem Gericht zu melden. Im Rahmen ihrer Aufgaben war die Staatsanwaltschaft an der Untersuchung und Verfolgung von Fällen von Polizeigewalt, Machtmissbrauch und Menschenrechtsverletzungen beteiligt. Darüber hinaus hat die Staatsanwaltschaft die Aufgabe, den Datenschutz zu überwachen, indem sie auf der Grundlage des verfassungsmäßigen Schutzes rechtliche Schritte einleitet oder sich daran beteiligt und neben der ANPD die Datenschutzrechte fördert. So trug die Staatsanwaltschaft beispielsweise dem Obersten Bundesgericht ihre Argumentation vor, die die Grundsatzentscheidung stützte, mit der der Datenschutz als Grundrecht in Brasilien anerkannt wurde²⁹⁷. Ein Register der Maßnahmen der Staatsanwaltschaft in Bezug auf das LGPD ist ebenfalls auf deren Website verfügbar²⁹⁸.

3.2.4. Rechtsbehelfe

- (197) Das brasilianische System bietet verschiedene gerichtliche und verwaltungsrechtliche Möglichkeiten, Rechtsschutz einschließlich Schadenersatz zu erlangen. Durch diese Mechanismen stehen betroffenen Personen wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe zur Verfügung, die es ihnen insbesondere ermöglichen, ihre Rechte durchzusetzen, unter anderem das Auskunftsrecht hinsichtlich ihrer personenbezogenen Daten oder das Recht auf Berichtigung oder Löschung dieser Daten.
- (198) Erstens können natürliche Personen vor Gericht Rechtsbehelfe einlegen und auch Schadenersatzansprüche geltend machen. Die Bundesverfassung und die Zivilprozessordnung bilden die Rechtsgrundlagen für die Geltendmachung von Schadenersatzansprüchen für materielle oder immaterielle Schäden, die durch die unrechtmäßige Erhebung oder Verwendung von Daten zu strafrechtlichen Zwecken durch eine Behörde verursacht wurden²⁹⁹. Insbesondere wird in der Verfassung ausdrücklich erwähnt, dass das Recht auf Privatsphäre ein „Recht auf Ersatz“ des

²⁹⁴ Artikel 127 der Verfassung der Föderativen Republik Brasilien von 1988.

²⁹⁵ Artikel 20 der EntschlieÙung 20 vom 28. Mai 2007, Externe Kontrolle der polizeilichen Tätigkeiten. Abrufbar unter: https://www.cnmp.mp.br/portal/images/Comissoes/CSP/Resolu%C3%A7%C3%B5es/_Resolu%C3%A7%C3%A3o_20.pdf.

²⁹⁶ Artikel 4 der EntschlieÙung 20 vom 28. Mai 2007, Externe Kontrolle der polizeilichen Tätigkeiten.

²⁹⁷ Siehe Erwägungsgrund 199 dieses Beschlusses und Oberstes Bundesgericht, Entscheidung in der Rechtssache ADI 6.387, Mai 2020. Abrufbar unter: <https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf>.

²⁹⁸ Staatsanwaltschaft, „Das LGPD bei der Staatsanwaltschaft“. Abrufbar unter: <https://www.mpf.mp.br/servicos/lgpd/lgpd-no-mpf>.

²⁹⁹ Siehe beispielsweise Artikel 43 des Gesetzes Nr. 10.408 vom 10. Januar 2002, Zivilprozessordnung. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm.

materiellen oder immateriellen Schadens umfasst, der sich aus seiner Verletzung ergibt³⁰⁰. Gegen Gerichtsentscheidungen können Rechtsmittel beim Obersten Bundesgericht und im Anschluss beim Interamerikanischen Gerichtshof für Menschenrechte eingelegt werden. Im Jahr 2009 wurde Brasilien vom Interamerikanischen Gerichtshof für Menschenrechte angewiesen, Beschäftigten von landwirtschaftlichen Genossenschaften eine Entschädigung zu zahlen, weil 1999 im Bundesstaat Paraná unter Verstoß gegen das Gesetz über die telefonische Überwachung und die Amerikanische Menschenrechtskonvention unzulässige Telefonüberwachungsmaßnahmen durchgeführt wurden³⁰¹.

- (199) Zweitens können sich natürliche Personen unabhängig von ihrer Staatsangehörigkeit auf den durch den Begriff der *Habeas Data* geschaffenen Schutz berufen, um weiterhin Zugang zu ihren bei Behörden gespeicherten Daten zu erhalten und diese berichtigen zu lassen³⁰². Auf dieser Grundlage können natürliche Personen auch vor Gericht Klage erheben, darunter „unmittelbare Verfassungsklagen“ (*Ação Direta de Inconstitucionalidade*, im Folgenden „ADI“) beim Obersten Bundesgericht. Das wegweisende Urteil des Obersten Bundesgerichts aus dem Jahr 2020, das in Brasilien den Weg für die Anerkennung des Datenschutzes als Grundrecht ebnet, ging auf ADI zurück, die auf der Grundlage des Grundsatzes *Habeas Data* eingereicht wurden³⁰³. Die Staatsanwaltschaft war ebenfalls an dem Verfahren beteiligt und unterstützte die Position der natürlichen Personen und der Zivilgesellschaft, die das Verfahren eingeleitet hatten. In der Rechtssache wurde eine Durchführungsverordnung angefochten, die darauf abzielte, während der COVID-19-Pandemie personenbezogene Daten von mehr als 200 Millionen Telekommunikationsteilnehmern an das brasilianische Institut für Geografie und Statistik weiterzugeben³⁰⁴. Das Oberste Bundesgericht stellte fest, dass die Durchführungsverordnung gegen die durch die Verfassung geschützten Grundrechte auf Privatsphäre und Vertraulichkeit der Kommunikation verstößt³⁰⁵. Die Durchführungsverordnung wurde ausgesetzt, und das Oberste Bundesgericht entschied, dass der Datenschutz als Grundrecht betrachtet und geschützt werden sollte, ähnlich wie das Recht auf Privatsphäre³⁰⁶. Zum Zeitpunkt der Entscheidung war das LGPD noch nicht in Kraft. Daher stützte sich das Richterergremium auf Rechtsvergleichung, insbesondere auf die Rechtsprechung des deutschen Bundesverfassungsgerichts und auf Artikel 8 der Charta der Grundrechte der Europäischen Union, um seine Auffassung über die Verfassungswidrigkeit der Durchführungsverordnung sowie die Auslegung der in der Verfassung garantierten Grundrechte auf Würde und Privatsphäre und die Anerkennung von *Habeas Data* als Instrument zum Schutz des Rechts auf informationelle Selbstbestimmung zu begründen³⁰⁷.

³⁰⁰ Artikel 5 Ziffer X der Verfassung der Föderativen Republik Brasilien von 1988.

³⁰¹ Interamerikanischer Gerichtshof für Menschenrechte, Rechtssache Escher u. a./Brasilien, Vorläufige Einwände, Begründetheit, Entschädigungen und Kosten. Urteil vom 6. Juli 2009. Abrufbar unter: http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf.

³⁰² Siehe Erwägungsgründe 9 und 161 dieses Beschlusses.

³⁰³ Oberstes Bundesgericht, Entscheidung in der Rechtssache ADI 6.387, Mai 2020. Abrufbar unter: <https://www.stf.jus.br/arquivo/cms/noticiario/stf/anexo/adi6387mc.pdf>.

³⁰⁴ Ausgesetzte Durchführungsverordnung Nr. 954 vom 17. April 2020. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm.

³⁰⁵ Oberstes Bundesgericht, Entscheidung in der Rechtssache ADI 6.387, Mai 2020, S. 12.

³⁰⁶ Oberstes Bundesgericht, Entscheidung in der Rechtssache ADI 6.387, Mai 2020, S. 8.

³⁰⁷ Siehe Oberstes Bundesgericht, Entscheidung in der Rechtssache ADI 6.387, Mai 2020, S. 4, und International Bar Association, The impact of Covid-19 for data protection in Brazil: the perspective of

- (200) Drittens können natürliche Personen gemäß Artikel 55-J Ziffer V und unter den in den Erwägungsgründen 146 und 149 dieses Beschlusses genannten Bedingungen bei der ANPD Rechtsbehelfe wegen eines Verstoßes gegen das LGPD einlegen. Sie können ihre im LGPD verankerten Datenschutzrechte auch gegenüber Behörden ausüben³⁰⁸.
- (201) Die in den Erwägungsgründen 197 bis 200 dieses Beschlusses beschriebenen Rechtsbehelfe stellen den betroffenen Personen wirksame verwaltungsrechtliche und gerichtliche Rechtsmittel zur Verfügung, die es ihnen insbesondere ermöglichen, ihre Rechte, einschließlich ihres Datenschutzrechts in Bezug auf solche Daten, durchzusetzen.
- 3.3. Zugriff und Verwendung durch brasilianische Behörden für die Zwecke der nationalen Sicherheit
- (202) Die Gesetze Brasiliens umfassen eine Reihe von Einschränkungen und Garantien in Bezug auf den Zugriff auf und die Verwendung von personenbezogenen Daten für die Zwecke der nationalen Sicherheit; ferner sehen sie Aufsichtsmechanismen und Rechtsbehelfe vor, die den in den Erwägungsgründen (156) bis (158) dieses Beschlusses genannten Anforderungen entsprechen. Die folgenden Abschnitte enthalten eine detaillierte Prüfung der Bedingungen, unter denen ein solcher Zugriff erfolgen kann, sowie der Garantien, die für die Nutzung dieser Befugnisse gelten.
- 3.3.1. Rechtsgrundlagen, Einschränkungen und Garantien
- (203) In Brasilien kann auf personenbezogene Daten für Zwecke der nationalen Sicherheit im Rahmen nachrichtendienstlicher Tätigkeiten auf der Grundlage des Gesetzes zur Einrichtung des brasilianischen Nachrichtendienstes (*Sistema Brasileiro de Inteligência*, im Folgenden „SISBIN“) zugegriffen werden³⁰⁹. Artikel 1 dieses Gesetzes sieht allgemein vor, dass der brasilianische Nachrichtendienst „die individuellen Rechte und Garantien sowie andere Bestimmungen der Bundesverfassung, Verträge, Übereinkommen, Übereinkünfte und internationale Verpflichtungen, deren Vertragspartei oder Unterzeichner die Föderative Republik Brasilien ist, beachten und wahren muss“³¹⁰. Dazu gehört die Gewährleistung der Grundsätze der Notwendigkeit und Verhältnismäßigkeit sowie des Rechts auf Datenschutz³¹¹. Die Tätigkeiten des brasilianischen Nachrichtendienstes werden in verbindlichen Erlassen näher beschrieben³¹².

Brazil's supreme court [Die Auswirkungen von COVID-19 auf den Datenschutz in Brasilien: die Sichtweise des Obersten Gerichts Brasiliens]. Abrufbar unter: <https://www.ibanet.org/article/82b25a81-7422-4f07-aaa8-9c2db19e22af#:~:text=On%206%20and%207%20May%202020%2C%20the,as%20an%20independent%20fundamental%20right%20in%20Brazil.&text=The%20processing%20of%20data%20is%20allowed%20only,legal%20principles%2C%20such%20as%20transparency%20and%20security.>

³⁰⁸ Artikel 23 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

³⁰⁹ Gesetz Nr. 9.883 vom 7. Dezember 1999. Gesetz zur Einrichtung des brasilianischen Nachrichtendienstes. Abrufbar unter: https://www.gov.br/mj/pt-br/acao-a-informacao/atuacao-internacional/legislacao-traduzida/lei-no-9-883-de-7-de-dezembro-de-1999_eng_rev-d.pdf.

³¹⁰ Artikel 1 Absatz 1 des Gesetzes Nr. 9.883 vom 7. Dezember 1999. Gesetz zur Einrichtung des brasilianischen Nachrichtendienstes.

³¹¹ Siehe Erwägungsgrund 160 dieses Beschlusses.

³¹² Erlass Nr. 8.793/2016 vom 29. Juni 2016 über die nationale Nachrichtendienstpolitik. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm sowie Erlass Nr. 4.376/2002 vom 13. September 2002 über die Organisation und Funktionsweise des brasilianischen Nachrichtendienstes. Abrufbar unter: https://www.gov.br/mj/pt-br/acao-a-informacao/atuacao-internacional/legislacao-traduzida/decreto-no-4-376-de-13-de-setembro-de-2002-seopi_eng_rev-d.pdf.

- (204) Nach Artikel 4 des Gesetzes zur Einrichtung des brasilianischen Nachrichtendienstes dürfen die zum SISBIN gehörenden Einrichtungen bestimmte Daten für Zwecke der nationalen Sicherheit („Segurança Pública“) erheben und analysieren. Der Begriff der „nationalen Sicherheit“ wird durch ein Gesetz aus dem Jahr 2021 geregelt, mit dem das Strafgesetzbuch geändert³¹³ und das brasilianische Gesetz über die nationale Sicherheit aufgehoben wurde³¹⁴. Mit dem Gesetz von 2021 wurde eine erschöpfende Liste von „Straftaten“ gegen die nationale Sicherheit festgelegt, die diesen Begriff umreißt. Bei diesen Straftaten handelt es sich um 1) „Straftaten gegen die „nationale Souveränität“ (darunter fallen Kriegshandlungen, eine Invasion in das Land, der Versuch, einen Teil des Staatsgebiets zu besetzen, um einen neuen Staat zu gründen, die Weitergabe von Verschlusssachen an ausländische Regierungen oder ausländische kriminelle Vereinigungen, die die verfassungsmäßige Ordnung der nationalen Souveränität gefährden könnten, und die Erleichterung oder Fälschung des Zugangs zu Informationssystemen für Unbefugte)³¹⁵, 2) Verbrechen gegen die „demokratischen Institutionen“ (darunter fallen der gewaltsame Versuch, die Rechtsstaatlichkeit durch die Verhinderung oder Einschränkung verfassungsmäßiger Befugnisse und durch einen Staatsstreich zu beenden)³¹⁶, 3) Verbrechen gegen die „Funktionsfähigkeit der demokratischen Institutionen während des Wahlprozesses“ (darunter fallen die Unterbrechung des Wahlprozesses und die gewaltsame Einschränkung oder Beeinträchtigung der Fähigkeit von natürlichen Personen, ihre politischen Rechte auszuüben)³¹⁷ und 4) Verbrechen gegen die Funktionsfähigkeit der wesentlichen Dienste (darunter fallen Sabotageakte gegen öffentliche Kommunikationsmittel und Verteidigungseinrichtungen mit dem Ziel, die Rechtsstaatlichkeit zu beenden)³¹⁸. In Artikel 359-T des Gesetzes wird klargestellt, dass die Ausübung des Rechts auf freie Meinungsäußerung, die verfassungsmäßigen Rechte und Befugnisse, die Ausübung journalistischer Tätigkeiten, einschließlich „durch Demonstrationen, Versammlungen, Streiks, Zusammenkünfte oder jede andere Form der politischen Demonstration mit sozialen Zielen“, nicht als Straftat angesehen werden dürfen³¹⁹. In der nationalen Nachrichtendienststrichtlinie Brasiliens wurde eine Reihe von Hauptzielen für die Nachrichtendienste festgelegt, die die Behörden berücksichtigen müssen, wie etwa die Verhinderung von „Sabotage“ oder „Spionage“³²⁰. Als „hochrangiges Orientierungsdokument“ wird mit der Nachrichtendienststrichtlinie jedoch weder die

³¹³ Gesetz Nr. 14.197 vom 1. September 2021 zur Änderung des Strafgesetzbuchs und zur Aufhebung des Gesetzes über die nationale Sicherheit von 1983. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14197.htm.

³¹⁴ Aufgehobenes Gesetz Nr. 7.170 vom 14. Dezember 1983 über die nationale Sicherheit. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/LEIS/L7170.htm.

³¹⁵ Kapitel I des Gesetzes Nr. 14.197 vom 1. September 2021 zur Änderung des Strafgesetzbuchs und zur Aufhebung des Gesetzes über die nationale Sicherheit von 1983.

³¹⁶ Kapitel II des Gesetzes Nr. 14.197 vom 1. September 2021 zur Änderung des Strafgesetzbuchs und zur Aufhebung des Gesetzes über die nationale Sicherheit von 1983.

³¹⁷ Kapitel III des Gesetzes Nr. 14.197 vom 1. September 2021 zur Änderung des Strafgesetzbuchs und zur Aufhebung des Gesetzes über die nationale Sicherheit von 1983.

³¹⁸ Kapitel IV des Gesetzes Nr. 14.197 vom 1. September 2021 zur Änderung des Strafgesetzbuchs und zur Aufhebung des Gesetzes über die nationale Sicherheit von 1983.

³¹⁹ Artikel 359-T des Gesetzes Nr. 14.197 vom 1. September 2021 zur Änderung des Strafgesetzbuchs und zur Aufhebung des Gesetzes über die nationale Sicherheit von 1983.

³²⁰ Artikel 3 des Erlasses Nr. 8.793/2016 vom 29. Juni 2016 über die nationale Nachrichtendienstpolitik. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm.

Liste der Straftaten im Zusammenhang mit dem Begriff der nationalen Sicherheit erweitert, noch wird die Definition der nationalen Sicherheit geändert³²¹.

- (205) Die Daten, auf die zugegriffen werden kann und die analysiert werden dürfen, um die oben aufgeführten Straftaten gegen die nationale Sicherheit zu verhindern, umfassen Informationen, auf die die Behörden, die zum SISBIN gehören, im Rahmen ihrer Tätigkeit und gemäß den in den Erwägungsgründen 165 bis 187 dieses Beschlusses beschriebenen Bedingungen (d. h. auf der Grundlage einer zu einem klar definierten Zweck erteilten richterlichen Genehmigung) zugreifen können. Die an SISBIN weitergegebenen Daten werden über ein sicheres verschlüsseltes elektronisches System mit Zugriffsprotokollen verarbeitet, um die Rückverfolgbarkeit und Überprüfbarkeit der Informationen sicherzustellen³²². Wie das Oberste Bundesgericht klargestellt hat, unterliegt die Weitergabe von Daten an SISBIN den Grundsätzen des LGPD, einschließlich der Zweckbindung (Artikel 6 Ziffer I LGPD), der Datenminimierung und Richtigkeit (Artikel 6 Ziffern III und V LGPD), der Transparenz (Artikel 6 Ziffer VI LGPD), der Datensicherheit (Artikel 6 Ziffer VII LGPD) und der Begrenzung der Speicherdauer (Artikel 6 Ziffern I, III, IV und Artikel 16 LGPD)³²³.
- (206) Artikel 2 des Gesetzes zur Einrichtung des brasilianischen Nachrichtendienstes besagt, dass nur öffentliche Behörden Teil dieses Systems sind. Zum SISBIN gehören der brasilianische Nachrichtendienst (*Agência Brasileira de Inteligência*, im Folgenden „ABIN“) und Vertreter von Nachrichtendiensten, Ministerien, Sekretariaten und Agenturen der Bundesverwaltung. Die Liste der Behörden, die zum SISBIN gehören, ist in einem Erlass über die Organisation und Funktionsweise des Systems festgelegt³²⁴.
- (207) Der ABIN ist das zentrale Organ des Nachrichtendienstes und für die Planung, Durchführung, Koordinierung, Überwachung und Kontrolle der nachrichtendienstlichen Tätigkeiten zuständig. Diese Tätigkeiten müssen mit vertraulichen Mitteln und Techniken durchgeführt werden, die auf Informationen beruhen. Zur Wahrnehmung seiner Aufgaben erhält der ABIN von den verschiedenen Behörden, die zum SISBIN gehören, spezifische Informationen und Daten, die die nationale Sicherheit betreffen. Die zum SISBIN gehörenden Behörden sind verpflichtet, diese Informationen zur Verfügung zu stellen³²⁵, da der ABIN nach dem Gesetz nicht befugt ist, Informationen selbst zu erheben. Die Rechtmäßigkeit der Verpflichtung zur Weitergabe von Daten durch die zum SISBIN gehörenden Behörden

³²¹ Einleitung, erster Absatz des Erlasses Nr. 8.793/2016 vom 29. Juni 2016 über die nationale Nachrichtendienstpolitik. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm.

³²² Siehe SISBIN-Broschüre, 2024, S. 18. Abrufbar unter: https://www.gov.br/abin/pt-br/institucional/sisbin/cart_ingles.pdf.

³²³ Oberstes Bundesgericht. Entscheidung in der Rechtssache ADI 6649, September 2022. Abrufbar unter: <https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false>.

³²⁴ Artikel 7 des Erlasses Nr. 11.693 vom 6. September 2023 über die Organisation und Funktionsweise des SISBIN. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm. Beispiele für die unter das SISBIN fallenden Behörden sind: das Nachrichtendienstzentrum des Verteidigungsministeriums, die Direktion Strafvollzugsaufklärung des Nationalen Sekretariats des Ministeriums für Justiz und öffentliche Sicherheit, das Generalsekretariat für Außenbeziehungen des Außenministeriums und die Direktion für Nachrichtendienste der Bundespolizei.

³²⁵ Artikel 4 des Gesetzes Nr. 9.883 vom 7. Dezember 1999. Gesetz zur Einrichtung des brasilianischen Nachrichtendienstes. Abrufbar unter: https://www.gov.br/mj/pt-br/acao-a-informacao/atualizacao-internacional/legislacao-traduzida/lei-no-9-883-de-7-de-dezembro-de-1999_eng_rev-d.pdf.

wurde vor dem Obersten Bundesgericht angefochten³²⁶. In seinem Urteil aus dem Jahr 2021 stellte das Oberste Bundesgericht klar, dass die Daten, die Behörden an den ABIN weitergeben, die strikten Zwecke des öffentlichen Interesses (z. B. Verteidigung öffentlicher Einrichtungen und nationaler Interessen) erfüllen müssen, und wies darauf hin, dass der spezifische und rechtmäßige Zweck jeder Tätigkeit der Datenweitergabe im Wege eines förmlichen Verfahrens festgelegt wird, das einer richterlichen Genehmigung unterliegt und in dieser festgelegt wird³²⁷. Diese Beschränkungen gelten auch für jede weitere Weitergabe von Daten zwischen Behörden³²⁸.

- (208) Schließlich muss die Verarbeitung von Daten im Sinne des SISBIN die Informationen vor dem Zugriff durch unbefugte Personen oder Stellen schützen. Artikel 5 des Erlasses über die Funktionsweise des SISBIN schreibt ausdrücklich vor, dass die Koordinierung und die Weitergabe von Daten zwischen den unter das System fallenden Stellen „den Rechtsvorschriften über das Berufsgeheimnis und die Sicherheit, den Schutz personenbezogener Daten und die Sicherheit von Informationen und Kenntnissen“ entsprechen müssen, zu denen das LGPD als wichtigstes Gesetz Brasiliens zum Schutz personenbezogener Daten gehört³²⁹. In Artikel 6 des Erlasses ist ferner festgelegt, dass die von den zum SISBIN gehörenden Behörden weitergegebenen Informationen „den Grundsätzen der Rechtssicherheit, der Notwendigkeit und des öffentlichen Interesses“ entsprechen und ein legitimes Ziel verfolgen müssen³³⁰. Im SISBIN wird auch anerkannt, wie wichtig es ist, das LGPD im Rahmen seiner öffentlichen Materialien und internen Verfahren einzuhalten³³¹.
- (209) Die Befugnisse der Behörden, die Daten für Zwecke der nationalen Sicherheit in Brasilien verarbeiten, sind daher durch klare und präzise gesetzlich vorgesehene Regeln begrenzt und unterliegen einer Reihe von Garantien. Diese Garantien umfassen insbesondere eine garantierte Überwachung der Durchführung solcher Maßnahmen, unter anderem durch vorherige richterliche Genehmigung und Schutzmaßnahmen zur Begrenzung des Zugangs zu den Informationen im Einklang mit den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit.

3.3.2. Weitere Verwendung der Daten

- (210) Die Verarbeitung personenbezogener Daten, die von brasilianischen Behörden zu Zwecken der nationalen Sicherheit erhoben werden, unterliegt den Grundsätzen der Zweckbindung (Artikel 6 Ziffer I LGPD), der Rechtmäßigkeit der Verarbeitung und Verarbeitung nach Treu und Glauben (Artikel 6 und 7 LGPD), der Datenminimierung und Richtigkeit (Artikel 6 Ziffern III und V LGPD), der Transparenz (Artikel 6 Ziffer VI LGPD), der Datensicherheit (Artikel 6 Ziffer VII LGPD) und der Begrenzung der Speicherdauer (Artikel 6 Ziffern I, III, IV und Artikel 16 LGPD).

³²⁶ Oberstes Bundesgericht, Entscheidung in der Rechtssache ADI 6529 vom 15. Oktober 2021. Abrufbar unter: <https://www.jusbrasil.com.br/jurisprudencia/stf/1303041724/inteiro-teor-1303041733>.

³²⁷ Oberstes Bundesgericht, Entscheidung in der Rechtssache ADI 6529 vom 15. Oktober 2021, S. 22.

³²⁸ Oberstes Bundesgericht, Entscheidung in der Rechtssache ADI 6529 vom 15. Oktober 2021, S. 3.

³²⁹ Artikel 5 des Erlasses Nr. 11.693 vom 6. September 2023 über die Organisation und Funktionsweise des SISBIN.

³³⁰ Artikel 6 des Erlasses Nr. 11.693 vom 6. September 2023 über die Organisation und Funktionsweise des SISBIN.

³³¹ Siehe beispielsweise SISBIN-Broschüre, S. 9: „Eines der Ziele dieser Neupositionierung besteht darin, die Rückverfolgbarkeit und Transparenz der internen Prozesse des SISBIN durch die Einführung von speziell für diese Zwecke entwickelten Instrumenten und digitalen Plattformen zu verbessern. Diese Instrumente müssen an den Rechtsrahmen angepasst werden, der durch das Gesetz über den Zugang zu Informationen und das Allgemeine Datenschutzgesetz (LGPD) geschaffen wurde, die beide 2012 erlassen wurden“. Abrufbar unter: https://www.gov.br/abin/pt-br/institucional/sisbin/cart_ingles.pdf.

- (211) Eine etwaige Weitergabe personenbezogener Daten an Dritte (einschließlich Drittländer und im Rahmen internationaler Übereinkünfte) kann nur im Einklang mit den Grundsätzen des LGPD erfolgen, nachdem die Einhaltung der Verfassungsgrundsätze der Notwendigkeit und Verhältnismäßigkeit geprüft und die Kontinuität des Schutzes und die Einhaltung der Rechte der betroffenen Personen sichergestellt wurden (Artikel 2 der Datenübermittlungsverordnung).

3.3.3. Aufsicht

- (212) Die Arbeit der brasilianischen nationalen Sicherheitsbehörden wird von verschiedenen Stellen überwacht. Im Erlass über die nationale nachrichtendienstliche Strategie Brasiliens wird auf die Bedeutung mehrerer Ebenen von Aufsichtsmechanismen zum Schutz der „demokratischen Rechtsstaatlichkeit“ hingewiesen³³². Das Oberste Bundesgericht wies auf die Bedeutung dieser Aufsicht in einem Fall hin, in dem es um die Verarbeitung von Daten im Rahmen des SISBIN ging, und stellte fest, dass „die Wirksamkeit nachrichtendienstlicher Tätigkeiten oft mit der Geheimhaltung des Prozesses und den erhobenen Informationen zusammenhängt. Im Bereich der demokratischen Rechtsstaatlichkeit unterliegt diese Funktion der externen Kontrolle durch die Gesetzgebung und die Gerichtsbarkeit, um zu beurteilen, ob die auferlegte Geheimhaltung den strengen öffentlichen Zielen, denen sie dient, angemessen ist“³³³.
- (213) Erstens gibt es eine Kontrolle durch die Exekutive, mit der sichergestellt wird, dass die vom Nachrichtendienst zu erreichenden Ziele sowie die umzusetzenden Strategien und die formulierten Pläne angemessen auf gesellschaftliche Anforderungen eingehen. Die Exekutive ist auch dafür verantwortlich, dass die Ausgaben der Nachrichtendienste vernünftig und ausschließlich für rechtmäßige, notwendige und nützliche Maßnahmen für den Staat getätigt werden. Im brasilianischen Rahmen wird diese Kontrolle von der Kammer für Außenbeziehungen und nationale Verteidigung des Regierungsrates ausgeübt, die für die Überwachung der Umsetzung der Nachrichtendienstpolitik zuständig ist, sowie vom institutionellen Sicherheitsbüro wahrgenommen, das für die Koordinierung der Tätigkeiten der Nachrichtendienste auf Bundesebene zuständig ist³³⁴.
- (214) Zweitens übt die Legislative die Kontrolle über die nachrichtendienstlichen Tätigkeiten aus. Der Zweck dieser Kontrolle besteht darin, sowohl die Rechtmäßigkeit als auch die Wirksamkeit der nachrichtendienstlichen Tätigkeit zu überprüfen. Die Vorsitzenden der Mehrheits- und Minderheitsparteien in der Abgeordnetenversammlung und im Bundessenat sowie die Vorsitzenden der Ausschüsse für Außenbeziehungen und Nationale Verteidigung der Abgeordnetenversammlung und des Bundessenats sind Teil des externen Aufsichtsgremiums für nachrichtendienstliche Tätigkeiten, dem Gemeinsamen Ausschuss für die Kontrolle nachrichtendienstlicher Tätigkeiten (*Comissão mista de Controle da Atividade de Inteligência*, im Folgenden „CCAI“)³³⁵. Die Kontrolle der Legislative über die nachrichtendienstlichen Tätigkeiten wurde im Jahr 1999 durch das Gesetz zur Einrichtung des brasilianischen Nachrichtendienstes festgelegt, und die Aufsichtsfunktion und die Befugnisse des CCAI wurden durch die

³³² Abschnitt 2.4 Absatz 4 des Erlasses vom 15. Dezember 2017 über eine nationale nachrichtendienstliche Strategie.

³³³ Oberstes Bundesgericht, Entscheidung vom 15. Oktober 2021, S. 2.

³³⁴ Abschnitt 2.4 des Erlasses vom 15. Dezember 2017 über eine nationale nachrichtendienstliche Strategie. Abrufbar unter: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/dsn/Dsn14503.htm.

³³⁵ Artikel 6 Absatz 1 des Gesetzes Nr. 9.883 vom 7. Dezember 1999. Gesetz zur Einrichtung des brasilianischen Nachrichtendienstes.

Annahme einer verbindlichen EntschlieÙung des Kongresses aus dem Jahr 2013³³⁶ erheblich gestärkt. Diese EntschlieÙung befasste sich mit zuvor festgestellten Mängeln bei der weiteren Institutionalisierung des CCAI, indem ihm eine ständige Struktur und ein Sekretariat zur Verfügung gestellt, Klarheit über seine Befugnisse geschaffen und die Transparenz seiner Tätigkeiten erhöht wurde. Die Rolle, die Tätigkeiten und die Befugnisse des CCAI sind in dieser EntschlieÙung und per Gesetz festgelegt. Der CCAI überwacht und kontrolliert die nachrichtendienstlichen Tätigkeiten von Einrichtungen der öffentlichen Verwaltung des Bundes, insbesondere der Einrichtungen, die dem SISBIN unterliegen, um sicherzustellen, dass die Tätigkeiten verfassungskonform durchgeführt werden, und um die Rechte und Garantien des Einzelnen, der Gesellschaft und des Staates zu schützen³³⁷. Der CCAI kann nachträgliche Überprüfungen, aber auch Prüfungen und Kontrollen laufender Tätigkeiten durchführen³³⁸. Die Mitglieder des CCAI verfügen über die höchste Zugangsberechtigung zu Dokumenten. Der CCAI erstellt Jahresberichte über seine Tätigkeiten, der jedoch keine Informationen enthält, die die nationale Sicherheit gefährden könnten³³⁹. Wie in Erwägungsgrund 222 dieses Beschlusses dargelegt, kann der CCAI auch Beschwerden von natürlichen Personen entgegennehmen und untersuchen.

- (215) Drittens überwacht die ANPD die Einhaltung der im LGPD festgelegten Parameter durch die nationalen Sicherheitsbehörden in Bezug auf die Verarbeitung personenbezogener Daten. Das LGPD gilt teilweise für die Verarbeitung personenbezogener Daten, die zum Zwecke der öffentlichen Sicherheit, der Landesverteidigung, der Staatssicherheit oder der Untersuchung und Verfolgung von Straftaten erfolgt³⁴⁰. In diesem Zusammenhang kann die ANPD ihre Untersuchungs- und Abhilfebefugnisse gemäß LGPD ausüben. Der ANPD kann beispielsweise jederzeit Prüfungen bei allen Behörden, einschließlich des Nachrichtendienstes, durchführen³⁴¹.
- (216) Schließlich entscheidet die Justiz über Klagen von Bürgerinnen und Bürgern gegen Behörden und kann in diesem Zusammenhang die Tätigkeiten überwachen, die aus Gründen der nationalen Sicherheit durchgeführt werden, um die Einhaltung aller verfassungsmäßigen Rechte und des einschlägigen Rechtsrahmens, einschließlich des LGPD, sicherzustellen. Gegen Gerichtsentscheidungen können Rechtsmittel beim Obersten Bundesgericht und im Anschluss beim Interamerikanischen Gerichtshof für Menschenrechte eingelegt werden.

³³⁶ EntschlieÙung Nr. 2 von 2021-CN über den Gemeinsamen Ausschuss für die Kontrolle nachrichtendienstlicher Tätigkeiten (CCAI). Abrufbar unter: <https://www2.camara.leg.br/legin/fed/rescon/2013/resolucao-2-22-novembro-2013-777449-publicacaooriginal-141944-pl.html>.

³³⁷ Abschnitt 2.4 des Erlasses vom 15. Dezember 2017 über eine nationale nachrichtendienstliche Strategie.

³³⁸ Siehe insbesondere Artikel 3 der EntschlieÙung Nr. 2 von 2021-CN über den Gemeinsamen Ausschuss für die Kontrolle nachrichtendienstlicher Tätigkeiten (CCAI).

³³⁹ Artikel 13 der EntschlieÙung Nr. 2 von 2021-CN zum Gemeinsamen Ausschuss für die Kontrolle nachrichtendienstlicher Tätigkeiten (CCAI). Informationen über Sitzungen und Dokumente des CCAI sind online verfügbar und werden regelmäßig aktualisiert. Abrufbar unter: <https://legis.senado.leg.br/atividade/comissoes/comissao/449/> and https://www.congressonacional.leg.br/legislacao-e-publicacoes/glossario-legislativo/-/legislativo/termo/comissao_mista_de_controle_das_atividades_de_inteligencia_ccai_cn.

³⁴⁰ Artikel 4 des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

³⁴¹ Artikel 55-J Ziffer XI des Gesetzes Nr. 13.709 vom 14. August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – Allgemeines Datenschutzgesetz.

3.3.4. Rechtsbehelfe

- (217) Das brasilianische System bietet verschiedene gerichtliche und verwaltungsrechtliche Möglichkeiten, Rechtsschutz einschließlich Schadenersatz zu erlangen. Durch diese Mechanismen stehen betroffenen Personen wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe zur Verfügung, die es ihnen insbesondere ermöglichen, ihre Rechte durchzusetzen, unter anderem das Auskunftsrecht hinsichtlich ihrer personenbezogenen Daten oder das Recht auf Berichtigung oder Löschung dieser Daten.
- (218) Wie in Erwägungsgrund 9 dieses Beschlusses dargelegt, ist der Zugang zu Rechtsbehelfen für brasilianische Staatsangehörige und Drittstaatsangehörige unabhängig davon, ob sie sich im Staatsgebiet aufhalten oder nicht, gewährleistet.
- (219) Erstens haben natürliche Personen ein „absolutes“ Recht, eine Klage zum Schutz ihrer Rechte einzureichen. Nach den allgemeinen Vorschriften der Zivilprozessordnung muss eine natürliche Person, um vor Gericht Klage erheben zu können, keinen Schaden nachweisen (d. h. sie muss nicht nachweisen, dass sie möglicherweise überwacht wird oder dass ihre Daten aus Gründen der nationalen Sicherheit verarbeitet wurden). Die natürliche Person kann ihre Rechte aus dem Grundsatz *Habeas Data* in Bezug auf von Nachrichtendiensten verarbeiteten Daten ausüben³⁴².
- (220) Natürliche Personen können Schadenersatz verlangen, wenn sie vor Gericht Rechtsmittel einlegen. Ebenso wie bei der Verarbeitung zu Strafverfolgungszwecken stellen die Bundesverfassung und die Zivilprozessordnung die Rechtsgrundlagen für die Geltendmachung von Ersatzansprüchen für materielle oder immaterielle Schäden dar, die von der Behörde verursacht wurden, die Daten unrechtmäßig erhoben oder genutzt hat, auch im Wege von Sammelklagen³⁴³.
- (221) Zweitens hat das Oberste Bundesgericht die teilweise Anwendung des LGPD auf Zwecke der nationalen Sicherheit und damit auch die Befugnisse der ANPD zur Bearbeitung von Beschwerden im Zusammenhang mit der Verarbeitung personenbezogener Daten durch Behörden aus Gründen der nationalen Sicherheit bestätigt³⁴⁴. In demselben Urteil stellte das Oberste Bundesgericht fest, dass gemäß Artikel 42 LGPD „die Verarbeitung personenbezogener Daten durch öffentliche Stellen, die gegen die gesetzlichen und verfassungsrechtlichen Vorgaben verstößt, die zivilrechtliche Haftung des Staates für Schäden, die der Person entstanden sind“ erfordert³⁴⁵.
- (222) Drittens kann der CCAI Beschwerden über Verstöße gegen Grundrechte und Garantien durch öffentliche Stellen und Einrichtungen, die nachrichtendienstliche und Spionageabwehrtätigkeiten ausüben, von allen Bürgerinnen und Bürgern, politischen

³⁴² Siehe Erwägungsgrund 9 dieses Beschlusses.

³⁴³ Siehe beispielsweise Artikel 43 des Gesetzes Nr. 10.408 vom 10. Januar 2002, Zivilprozessordnung. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm und Artikel 1 des Gesetzes Nr. 7.397 vom 24. Juli 1985 über die zivilrechtliche Verantwortung. Abrufbar unter: https://www.planalto.gov.br/ccivil_03/leis/17347orig.htm.

³⁴⁴ Siehe Erwägungsgründe 31 und 162 dieses Beschlusses und Oberstes Bundesgericht, Entscheidung in der Rechtssache ADI 6649 vom 15. September 2022. Abrufbar unter: <https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false>.

³⁴⁵ Oberstes Bundesgericht, Entscheidung in der Rechtssache ADI 6649 vom 15. September 2022, Nr. 8. Abrufbar unter: <https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false>.

Parteien oder Vereinigungen entgegennehmen und untersuchen³⁴⁶. Auf dieser Grundlage kann der CCAI Kontrollen oder Untersuchungen durchführen. Der CCAI bietet daher einen zusätzlichen administrativen Rechtsbehelf für den Fall von Rechtsverletzungen im Zusammenhang mit der Verarbeitung von Daten zu Zwecken der nationalen Sicherheit. Die beim CCAI eingegangenen Beschwerden können anschließend an die Gerichte weitergeleitet werden.

- (223) Die verschiedenen Rechtsbehelfe, die im Rahmen des brasilianischen Rechtssystems zur Verfügung stehen, ermöglichen es natürlichen Personen, Rechtsmittel einzulegen. Insbesondere können natürliche Personen die Rechtmäßigkeit von Maßnahmen öffentlicher Behörden und von Nachrichtendiensten anfechten. Darüber hinaus können sie Schadenersatz erhalten.

4. SCHLUSSFOLGERUNG

- (224) Die Kommission ist der Ansicht, dass die Föderative Republik Brasilien durch ihr allgemeines Datenschutzgesetz (LGPD) ein Schutzniveau für aus der Europäischen Union übermittelte personenbezogene Daten gewährleistet, das der Sache nach dem durch die Verordnung (EU) 2016/679 garantierten Schutzniveau gleichwertig ist.
- (225) Darüber hinaus ist die Kommission der Auffassung, dass die Aufsichtsmechanismen und Rechtsbehelfe im brasilianischen Recht es insgesamt ermöglichen, etwaige Verstöße gegen die Datenschutzvorschriften durch Datenverantwortliche und Auftragsverarbeiter in Brasilien zu erkennen und in der Praxis zu bekämpfen und der betroffenen Person Rechtsbehelfe zur Verfügung zu stellen, um Auskunft über ihre personenbezogenen Daten zu erhalten und schließlich die Berichtigung oder Löschung dieser Daten zu erwirken.
- (226) Schließlich ist die Kommission auf der Grundlage der verfügbaren Informationen über die brasilianische Rechtsordnung der Auffassung, dass jeder Eingriff in die Grundrechte der natürlichen Personen, deren personenbezogene Daten aus der Europäischen Union an Brasilien übermittelt werden, durch brasilianische Behörden aus Gründen des öffentlichen Interesses, insbesondere zu Zwecken der Strafverfolgung und der nationalen Sicherheit, auf das zur Erreichung des betreffenden berechtigten Ziels unbedingt erforderliche Maß beschränkt ist und dass ein wirksamer Rechtsschutz gegen solche Eingriffe besteht.
- (227) In Anbetracht der in diesem Beschluss getroffenen Feststellungen sollte daher beschlossen werden, dass Brasilien ein angemessenes Schutzniveau im Sinne des Artikels 45 der Verordnung (EU) 2016/679, ausgelegt im Lichte der Charta der Grundrechte der Europäischen Union, für personenbezogene Daten gewährleistet, die aus der Europäischen Union an für die Verarbeitung Verantwortliche und Auftragsverarbeiter in Brasilien, die dem LGPD unterliegen, übermittelt werden.

5. AUSWIRKUNGEN DIESES BESCHLUSSES UND MASSNAHMEN DER DATENSCHUTZBEHÖRDEN

- (228) Die Mitgliedstaaten und ihre Organe müssen die notwendigen Maßnahmen treffen, um Rechtsakten der Unionsorgane nachzukommen, da für diese Rechtsakte eine Vermutung der Rechtmäßigkeit gilt, sodass sie Rechtswirkungen entfalten, solange sie nicht zurückgenommen, im Rahmen einer Nichtigkeitsklage für nichtig erklärt oder

³⁴⁶ Artikel 3 Ziffer XI der EntschlieÙung Nr. 2 von 2021-CN zum Gemeinsamen Ausschuss für die Kontrolle nachrichtendienstlicher Tätigkeiten („Comissão mista de Controle da Atividade de Inteligência – CCAI“).

infolge eines Vorabentscheidungsersuchens oder einer Einrede der Rechtswidrigkeit für ungültig erklärt wurden.

- (229) Daher ist ein nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 erlassener Angemessenheitsbeschluss der Kommission für alle Organe der Mitgliedstaaten, an die er gerichtet ist, einschließlich ihrer unabhängigen Aufsichtsbehörden, verbindlich. So können insbesondere Übermittlungen von einem Verantwortlichen oder Auftragsverarbeiter in der Europäischen Union an Datenverantwortliche und Auftragsverarbeiter in Brasilien ohne weitere Genehmigung vorgenommen werden.
- (230) Es sei daran erinnert, dass gemäß Artikel 58 Absatz 5 der Verordnung (EU) 2016/679 und wie vom Gerichtshof der Europäischen Union im Urteil in der Rechtssache Schrems erläutert Folgendes gilt: Wenn eine nationale Datenschutzbehörde, auch auf eine Beschwerde hin, die Vereinbarkeit eines Angemessenheitsbeschlusses der Kommission mit den Grundrechten des Einzelnen auf Privatsphäre und Datenschutz infrage stellt, muss das nationale Recht Rechtsbehelfe vorsehen, die es der Datenschutzbehörde ermöglichen, diese Beschwerden vor einem nationalen Gericht geltend zu machen, das gegebenenfalls ein Vorabentscheidungsverfahren beim Gerichtshof einleiten muss³⁴⁷.

6. ÜBERWACHUNG, AUSSETZUNG, AUFHEBUNG ODER ÄNDERUNG DIESES BESCHLUSSES

- (231) Nach der Rechtsprechung des Gerichtshofs³⁴⁸ und Artikel 45 Absatz 4 der Verordnung (EU) 2016/679 sollte die Kommission nach Erlass eines Angemessenheitsbeschlusses die maßgeblichen Entwicklungen in dem Drittland fortlaufend überwachen, um festzustellen, ob ein Drittland weiterhin ein im Wesentlichen gleichwertiges Schutzniveau bietet. Eine solche Kontrolle ist auf jeden Fall erforderlich, wenn der Kommission Informationen vorliegen, die Anlass zu begründeten Zweifeln geben.
- (232) Daher sollte die Kommission die Situation in Brasilien in Bezug auf den Rechtsrahmen und die tatsächliche Praxis bei der Verarbeitung personenbezogener Daten, wie in diesem Beschluss geprüft, fortlaufend überwachen. In dieser Hinsicht sollte besonders auf die Anwendung der Anforderungen an die Folgenabschätzung für den Datenschutz in der Praxis geachtet werden, auf die Transparenzanforderungen und deren etwaige Beschränkungen in Bezug auf das Recht auf Information und Zugang, auf die Vorschriften über die Meldung von Verletzungen des Schutzes personenbezogener Daten, auf die Sanktionsregelung sowie auf die Einhaltung der Beschränkungen und Garantien in Bezug auf den staatlichen Zugriff, wobei alle einschlägigen Entwicklungen in dieser Hinsicht zu berücksichtigen sind.
- (233) Um diesen Überwachungsprozess zu erleichtern, werden die brasilianischen Behörden, einschließlich der ANPD, ersucht, die Kommission über wesentliche Entwicklungen im Zusammenhang mit diesem Beschluss zu unterrichten, und zwar in Bezug auf die Verarbeitung personenbezogener Daten durch Unternehmer und Behörden sowie hinsichtlich der Einschränkungen und Garantien, die für den Zugriff der Behörden auf personenbezogene Daten gelten.

³⁴⁷ Schrems I, Rn. 65. „Insoweit ist es Sache des nationalen Gesetzgebers, Rechtsbehelfe vorzusehen, die es der betreffenden nationalen Kontrollstelle ermöglichen, die von ihr für begründet erachteten Rügen vor den nationalen Gerichten geltend zu machen, damit diese, wenn sie die Zweifel der Kontrollstelle an der Gültigkeit der Entscheidung der Kommission teilen, um eine Vorabentscheidung über deren Gültigkeit ersuchen.“

³⁴⁸ Schrems I, Rn. 76.

- (234) Damit die Kommission ihre Überwachungsfunktion wirksam ausüben kann, sollten die Mitgliedstaaten die Kommission über alle relevanten Maßnahmen der nationalen Datenschutzbehörden informieren, insbesondere über Anfragen oder Beschwerden von betroffenen EU-Bürgern in Bezug auf die Übermittlung personenbezogener Daten aus der Europäischen Union an Datenverantwortliche und Auftragsverarbeiter in Brasilien. Ferner sollte die Kommission über jegliche Hinweise informiert werden, die darauf hindeuten, dass die Maßnahmen der brasilianischen Behörden, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder für die nationale Sicherheit zuständig sind, einschließlich der Aufsichtsbehörden, nicht das erforderliche Schutzniveau gewährleisten.
- (235) In Anwendung des Artikels 45 Absatz 3 der Verordnung (EU) 2016/679³⁴⁹ und angesichts der Tatsache, dass sich das von der brasilianischen Rechtsordnung gewährte Schutzniveau ändern könnte, sollte die Kommission nach der Annahme dieses Beschlusses regelmäßig prüfen, ob die Feststellungen über die Angemessenheit des durch Brasilien gewährleisteten Schutzniveaus noch sachlich und rechtlich gerechtfertigt sind.
- (236) Zu diesem Zweck sollte dieser Beschluss innerhalb von vier Jahren nach seinem Inkrafttreten einer ersten Überprüfung unterzogen werden. Die anschließenden regelmäßigen Überprüfungen sollten mindestens alle vier Jahre stattfinden³⁵⁰. Die Überprüfungen sollten sich auf alle Aspekte der Funktionsweise dieses Beschlusses erstrecken, einschließlich der Zusammenarbeit der ANPD mit den Datenschutzbehörden der EU bei Beschwerden von natürlichen Personen. Sie sollte sich auch auf die Wirksamkeit der Aufsicht und Durchsetzung im Bereich der Strafverfolgung und der nationalen Sicherheit erstrecken.
- (237) Zur Durchführung der Überprüfung sollte die Kommission mit der ANPD zusammenkommen, gegebenenfalls unter Mitwirkung anderer brasilianischer Behörden, die für den staatlichen Zugriff zuständig sind, einschließlich der zuständigen Aufsichtsbehörden. Die Teilnahme an dieser Zusammenkunft sollte Vertretern der Mitglieder des Europäischen Datenschutzausschusses offenstehen. Im Rahmen der Überprüfung sollte die Kommission die ANPD ersuchen, umfassende Informationen über alle Aspekte, die für die Feststellung der Angemessenheit von Belang sind, vorzulegen, auch über die Einschränkungen und Garantien in Bezug auf den staatlichen Zugriff. Die Kommission sollte auch Erläuterungen zu allen für diesen Beschluss maßgeblichen, ihr vorliegenden Informationen einholen, einschließlich öffentlicher Berichte von brasilianischen Behörden oder anderen Beteiligten in Brasilien, dem Europäischen Datenschutzausschuss, einzelnen Datenschutzbehörden, zivilgesellschaftlichen Gruppen, Medienberichten oder jeder anderen verfügbaren Informationsquelle.
- (238) Auf der Grundlage der Überprüfung sollte die Kommission einen öffentlichen Bericht erstellen, der dem Europäischen Parlament und dem Rat vorgelegt wird.
- (239) Lassen verfügbare Informationen – insbesondere Informationen, die sich aus der Überwachung dieses Beschlusses ergeben oder von den Behörden Brasiliens oder der

³⁴⁹ Nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 ist „[i]n dem Durchführungsrechtsakt ... ein Mechanismus für eine regelmäßige Überprüfung, ... vorzusehen, bei der allen maßgeblichen Entwicklungen in dem Drittland oder bei der internationalen Organisation Rechnung getragen wird.“

³⁵⁰ Nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 muss „mindestens alle vier Jahre eine regelmäßige Überprüfung stattfinden“. Siehe auch Europäischer Datenschutzausschuss, Referenzgrundlage für Angemessenheit, WP 254 Rev. 01.

Mitgliedstaaten zur Verfügung gestellt werden – darauf schließen, dass das durch Brasilien gewährleistete Schutzniveau möglicherweise nicht mehr angemessen ist, sollte die Kommission die zuständigen Behörden Brasiliens davon in Kenntnis setzen und sie auffordern, innerhalb einer bestimmten, angemessenen Frist geeignete Maßnahmen zu ergreifen.

- (240) Falls die zuständigen brasilianischen Behörden nach Ablauf dieser Frist keine derartigen Maßnahmen ergriffen haben oder nicht auf andere Weise glaubhaft gemacht haben, dass dieser Beschluss weiterhin auf einem angemessenen Schutzniveau beruht, wird die Kommission das Verfahren gemäß Artikel 93 Absatz 2 der Verordnung (EU) 2016/679 einleiten, um diesen Beschluss teilweise oder vollständig auszusetzen oder aufzuheben.
- (241) Alternativ wird die Kommission dieses Verfahren einleiten, um den Beschluss zu ändern, indem sie insbesondere Datenübermittlungen zusätzlichen Bedingungen unterwirft oder den Anwendungsbereich der Angemessenheitsfeststellung auf Datenübermittlungen beschränkt, für die auch weiterhin ein angemessenes Schutzniveau gewährleistet ist.
- (242) Die Kommission sollte ferner die Einleitung des Verfahrens zur Änderung, Aussetzung oder Aufhebung dieses Beschlusses in Betracht ziehen, wenn die zuständigen brasilianischen Behörden im Rahmen der Überprüfung oder anderweitig nicht die Informationen oder Erläuterungen liefern, die für die Bewertung des Schutzniveaus für personenbezogene Daten, die aus der Europäischen Union nach Brasilien übermittelt werden, oder für die Einhaltung dieses Beschlusses erforderlich sind. In diesem Zusammenhang sollte die Kommission Überlegungen dazu anstellen, inwieweit die relevanten Informationen aus anderen Quellen bezogen werden können.
- (243) In hinreichend begründeten Fällen äußerster Dringlichkeit wird die Kommission von der Möglichkeit Gebrauch machen, nach dem in Artikel 93 Absatz 3 der Verordnung (EU) 2016/679 genannten Verfahren sofort geltende Durchführungsrechtsakte zur Aussetzung, Aufhebung oder Änderung des Beschlusses zu erlassen.

7. SCHLUSSBEMERKUNGEN

- (244) Der Europäische Datenschutzausschuss hat seine Stellungnahme veröffentlicht³⁵¹, der bei der Ausarbeitung dieses Beschlusses Rechnung getragen wurde.
- (245) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des gemäß Artikel 93 Absatz 1 der Verordnung (EU) 2016/679 eingesetzten Ausschusses —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Für die Zwecke des Artikels 45 der Verordnung (EU) 2016/679 gewährleistet Brasilien ein angemessenes Schutzniveau für personenbezogene Daten, die aus der Europäischen Union an Verantwortliche und Auftragsverarbeiter in Brasilien übermittelt werden, die dem Allgemeinen Datenschutzgesetz (LGPD) unterliegen.

³⁵¹ Europäischer Datenschutzausschuss, Stellungnahme zu einem Angemessenheitsbeschluss in Bezug auf Brasilien, November 2025. Abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-282025-regarding-european-commission-draft_de.

Artikel 2

Üben die zuständigen Behörden in den Mitgliedstaaten zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten ihre Befugnisse nach Artikel 58 der Verordnung (EU) 2016/679 im Hinblick auf die Übermittlung von Daten im Rahmen des Anwendungsbereichs gemäß Artikel 1 aus, so unterrichtet der betreffende Mitgliedstaat unverzüglich die Kommission.

Artikel 3

- (1) Die Kommission überwacht kontinuierlich die Anwendung des Rechtsrahmens, auf den sich dieser Beschluss stützt, um zu beurteilen, ob Brasilien weiterhin ein angemessenes Schutzniveau im Sinne des Artikels 1 gewährleistet.
- (2) Die Mitgliedstaaten und die Kommission unterrichten einander über Fälle, in denen die brasilianische Datenschutzbehörde (*Agência Nacional de Proteção de Dados – ANPD*) oder eine andere zuständige brasilianische Behörde die Einhaltung des Rechtsrahmens, auf den sich dieser Beschluss stützt, nicht gewährleistet.
- (3) Die Mitgliedstaaten und die Kommission unterrichten einander über Hinweise darauf, dass Eingriffe brasilianischer Behörden in das Recht von natürlichen Personen auf Schutz ihrer personenbezogenen Daten über den unbedingt erforderlichen Umfang hinausgehen oder dass es keinen wirksamen Rechtsschutz gegen solche Eingriffe gibt.
- (4) Vier Jahre nach dem Tag der Bekanntgabe dieses Beschlusses an die Mitgliedstaaten und danach mindestens alle vier Jahre evaluiert die Kommission die Feststellung in Artikel 1 auf der Grundlage aller verfügbaren Informationen, einschließlich der Informationen, die sie im Rahmen der mit den zuständigen brasilianischen Behörden durchgeführten Überprüfung erhalten hat.
- (5) Liegen der Kommission Hinweise darauf vor, dass ein angemessenes Schutzniveau nicht mehr gewährleistet ist, so unterrichtet sie die zuständigen Behörden Brasiliens und kann diesen Beschluss aussetzen, aufheben oder ändern.
- (6) Die Kommission kann diesen Beschluss auch aussetzen, aufheben oder ändern, wenn sie aufgrund mangelnder Kooperation der Regierung Brasiliens nicht feststellen kann, ob die Feststellung in Artikel 1 dieses Beschlusses berührt ist.

Artikel 4

Dieser Beschluss ist an die Mitgliedstaaten gerichtet.

Brüssel, den 26.1.2026

*Für die Kommission
Michael McGRATH
Mitglied der Kommission*

