Internationale Arbeitsgruppe
zum Datenschutz
in der Telekommunikation

675.56.12

Arbeitspapier zu

Standards für den Datenschutz und den Schutz der Privatsphäre bei grenzüberschreitenden Datenanforderungen zu Strafverfolgungszwecken

63. Sitzung, 9.-10. April 2018, Budapest (Ungarn)

Da Daten zunehmend in der ganzen Welt ausgetauscht und gespeichert werden, ist die Rechtsdurchsetzung ebenfalls zu einem internationalen Unterfangen geworden. Die Strafverfolgungsbehörden bemühen sich bei strafrechtlichen Ermittlungen zunehmend um den Zugang zu personenbezogenen Daten, die sich außerhalb ihrer Landesgrenzen befinden. Allerdings werfen diese Anfragen schwierige Fragen im Hinblick auf die Einhaltung nationaler und internationaler Standards zum Daten- und Privatsphärenschutz.

Traditionelle Regelungen zur Abwicklung grenzüberschreitender Datenanfragen in Strafsachen – durch Rechtshilfeabkommen (MLAT) – können einen gewissen Schutz bieten. MLATs erleichtern die internationale Zusammenarbeit der Strafverfolgungsbehörden und reduzieren Konflikte, sorgen für einen kohärenten Prozess der Aufsicht und tragen dazu bei, dass die Offiziellen geeignete legale Kanäle nutzen, um personenbezogene Daten anzufordern, und verringern das rechtliche Risiko für Unternehmen. [1] Allerdings gilt das MLAT-System, so wie es derzeit funktioniert, durch die zunehmende Häufigkeit und Komplexität grenzüberschreitender Datenanfragen als überlastet. Die Entschlüsselung und Erfüllung der jeweiligen Anforderungen an die Autorisierung des Datenzugriffs in den einzelnen Rechtssystemen stellen offenbar eine Herausforderung dar.[2] Auch sind die Stellen,

[1] *Siehe z. B.* Abkommen über Rechtshilfe zwischen der Europäischen Union und den Vereinigten Staaten von Amerika, 2003 OJ (L181) 34 („routing requests“ durch “central authorities” zur Überprüfung, einschließlich Artikel 9 “Limitations on use to protect personal and other data”).

[2] Gail Kent, *Sharing Investigation-Specific Data with Law Enforcement-An International Approach* 7 (Feb. 14, 2014) („Stanford Public Law Working Paper“) („The Central Authorities’ burden is further increased by the variety of standards of request that are received…. few countries have national policies or procedures that ensure requests or responses to MLAT requests meet the necessary legal or administrative standards for the other country, which may include specialist language”, referencing U.S. “probable cause” standard as an example).

Sekretariat
Berliner Beaufte für
Datenschutz und Informationsarbeit
Friedrichstr.219
D — 10969 Berlin
Telefon + 49/30/13889 0
Fax: + 49/30/215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http: //www.berlin-privacy-group.org

Die Arbeitsgruppe wurde eingeleitet
von den Datenschutzbeauftragten
aus verschiedenen Ländern
Verbesserung der Privatsphäre und des
Datenschutzes
in den Bereichen Telekommunikation
und Medien

die solche Anfragen bearbeiten, häufig unterfinanziert und personell unterbesetzt.[3] Infolgedessen kann es zu erheblichen Verzögerungen bei der Bearbeitung von Anträgen kommen, und eine Beantwortung des Antrags, einmal eingegangen, ist möglicherweise nicht ausreichend. Darüber hinaus unterliegen bestimmte Länder und Datenquellen keinem MLAT.

Darüber hinaus können sogar offizielle grenzüberschreitende Übertragungsmechanismen undurchsichtig sein. Nicht alle Länder melden eindeutige aggregierte statistische Daten zum MLAT-Prozess. Alternative Regelungen für die Übermittlung solcher Daten, wie z. B. freiwillige Vereinbarungen zwischen Diensteanbietern und ausländischen Regierungen, können unterschiedlichen oder unbekannten Standards unterworfen sein, keine Rechtskraft haben und daher wenig Sicherheit für den Schutz der Rechte der betroffenen Personen bieten.

Diese Herausforderungen bei der Durchführung grenzüberschreitender Datenanfragen stellen einen Anreiz für die Regierungen dar, auf andere Mechanismen zurückzugreifen. Mehrere Länder haben einseitig Befugnisse ausgeübt, um Unternehmen dazu zu zwingen, Daten zu produzieren, auch wenn die Daten in einem anderen Staat aufbewahrt werden. Zum Beispiel haben die USA versucht, von Microsoft E-Mail-Inhalte zu erlangen, die in Irland gespeichert waren.[4] Ein US-Berufungsgericht entschied, dass das US-Recht keine Befugnisse für die Durchsuchung und Beschlagnahme von E-Mail-Inhalten, die auf ausländischen Servern gespeichert sind, zulässt; zwar wurde der Fall dem US Supreme Court vorgelegt, die Parteien einigten sich jedoch, die Klage als akademisch abzuweisen, nachdem der "CLOUD Act" verabschiedet worden war, der den Zugriff der Strafverfolgungsbehörden auf Daten unabhängig vom Speicherort erlaubt.[5] Wiederum andere Behörden haben Unternehmen aufgefordert, Daten bereitzustellen, die außerhalb der Staatsgrenzen liegen. Angesichts des Risikos, gegen den U.S. Stored Communications Act, der die Offenlegung von Kommunikationsinhalten einschränkt, zu verstoßen, weigerte sich die brasilianische Tochtergesellschaft von Microsoft in den USA gespeicherte Daten zu übergeben und wurde durch brasilianische Behörden mit einer Geldbuße belegt und ein lokaler Mitarbeiter wurde von brasilianischen Behörden strafrechtlich belangt.[6] Im Jahr 2015 verhängte ein Gericht in Belgien ebenfalls eine Geldstrafe gegen Yahoo wegen der Nichtvorlage von IP-Adressen im Zusammenhang mit einer strafrechtlichen Ermittlung.[7] Die chinesischen Justizbehörden gestatten nun eine gewisse Fernextraktion (Kopieren) von Daten außerhalb des chinesischen Festlands, wenn es nicht möglich ist, das ursprüngliche Speichermaterial zu beschlagnahmen.[8]

---

[3] *Siehe z.* B. U.S. Department of Justice, FY 2019 Budget Request - General Legal Activities, Criminal Division 2 (mit dem Hinweis auf die Notwendigkeit weiterer personeller und finanzieller Mittel zur Deckung des „gegenwärtigen und wachsenden“ Bedarfs des Office of International Affairs und der MLAT-Prozesse).

[4] *United States v. Microsoft Corp.* ,138 S. Ct.1186 (2018).

[5] *ebenda*

[6] *International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests: Hearing Before the H. Comm. On the Judiciary,* 114th Cong.(2016) (schriftliche Aussage des Präsidenten und Chief Legal Officer von Microsoft, Brad Smith);*Siehe auch* „Marco Civil“ (Law 12965/2014), Art. 11, Abs. 2 (Anwendung des brasilianischen Rechts auf ausländische Internet-Unternehmen, die Dienstleistungen in Brasilien anbieten oder einen Angestellten mit Sitz in Brasilien haben).

[7] Hof van Cassatie [Belgisches Kassationsgericht], 1. Dezember 2015, Pas. 13.2082 N, No. 7, 485 (Belg.) [Englische Übersetzung abrufbar unter http: //journals.sas.ac.uk/deeslr/article/viewFile/2310/2261].

[8] *On the handling of criminal cases to collect and review the provisions of a number of issues to determine the electronic data* (Erlass des Supreme People's Court, Supreme People's Procuratorate, Ministry of Public Security, Sept. 20, 2016), http: //www.spp.gov.cn/xwfbh/wsfbt/201609/t20160920_167380_1.shtml.

Aktuelle Entwicklungen

Artikel 32 des Übereinkommens des Europarats über Computerkriminalität („Budapest Convention") sieht bestimmten „Grenzüberschreitenden Zugriff auf gespeicherte Computerdaten" vor, „mit Zustimmung oder wenn diese öffentlich zugänglich sind".[9] Auf nationaler Ebene erfordert Art. 18, dass die Parteien des Übereinkommens ihre Behörden ermächtigen anzuordnen, „dass eine Person in ihrem Hoheitsgebiet bestimmte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden und die in einem Computersystem oder auf einem Computerdatenträger gespeichert sind", und „dass ein Diensteanbieter, der seine Dienste im Hoheitsgebiet der Vertragspartei anbietet, Bestandsdaten in Zusammenhang mit diesen Diensten, die sich in seinem Besitz oder unter seiner Kontrolle befinden", vorzulegen hat. Der Ausschuss des Europarats für Cyberkriminalität (Cyber Crime Committee, T-CY), der die Vertragsstaaten des Budapester Übereinkommens vertritt, hat den grenzüberschreitenden Zugang zu Cloud-Daten als hohe Priorität ausgewiesen und sieht Änderungsbedarf.[10] Daher hat sich der Ausschuss im Juni 2017 auf ein Mandat für die Ausarbeitung von Zielvorgaben für die Vorbereitung eines Entwurfs eines zweiten Zusatzprotokolls zum Budapester Übereinkommen über Computerkriminalität verständigt, um die internationale Zusammenarbeit zu verstärken.[11] Dieses soll Bestimmungen mit einbeziehen über eine effizientere Rechtshilfe, klarere Rahmenbedingungen und Garantien, einschließlich Datenschutzanforderungen, aber auch die Kodifizierung bestehender Praktiken und Bestimmungen enthalten über die direkte Zusammenarbeit mit Diensteanbietern in anderen Rechtsräumen.

Die Europäische Kommission hat im Juni 2017 ein informelles Diskussionspapier zum Thema „Verbesserung des grenzüberschreitenden Zugriffs auf elektronische Beweismittel in Strafsachen" (keine offizielle Übersetzung)[12] vorgelegt und eine öffentliche Konsultation zu dieser Frage eingeleitet, die Ende Oktober 2017 abgeschlossen wurde. Die Initiative der Kommission „zielt darauf ab, Hindernisse für den grenzüberschreitenden Zugang zu elektronischen Beweismitteln in strafrechtlichen Ermittlungen zu beseitigen" (keine offizielle Übersetzung)[13], wozu auch Überlegungen gehören, Diensteanbieter, die außerhalb der Europäischen Union ihren Sitz haben, unabhängig von etwaigen geltenden MLATs oder anderen internationalen Übereinkünften unmittelbar zu verpflichten. Die Kommission beabsichtigt, Anfang 2018 einen konkreten Legislativvorschlag vorzulegen.[14]

---

[9] Übereinkommen des Europarates über Computerkriminalität, 23. November 2001, Europ. T.S. Nr. 185, Art.32, https: //rm.coe.int/1680081561.

[10] *Siehe z. B.* Cybercrime Convention Committee*, Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime* (2017), https: //rm.coe.int/terms-of-reference-for-the-preparation-ofa-draft-2nd-additional-proto/168072362b. S*iehe auch:* Cybercrime Convention Committee, *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY (2016),* https://rm.coe.int/16806a495e (Bericht der T-CY Cloud Evidence Group).

[11] *Siehe oben*, Cybercrime Convention Committee, *Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime (2017).*

[12] Commission Services, *Improving Cross-border Access to Electronic Evidence: Findings from the Expert Process and Suggested Way Forward, (2017)*, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf.

[13] Europäische Kommission, *Inception Impact Assessment (2017)*, https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en.

[14] Europäische Kommission, Migration & Inneres, e-evidence, https: //ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en. Am 17. April 2017 hat die Europäische Kommission schließlich eine „Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen" (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN) sowie eine „Richtlinie des Europäischen Parla-

In einer Pressemitteilung und einer „Erklärung zu elektronischen Beweismitteln“ (keine offizielle deutsche Übersetzung) hat die Art. 29-Datenschutzgruppe „mehrere Bedenken und Vorbehalte zu den von der Europäischen Kommission in Erwägung gezogenen legislativen Optionen“ (keine offizielle deutsche Übersetzung) geäußert.[15] Die Arbeitsgruppe hat ferner auf die Notwendigkeit hingewiesen, „dass der künftige Gesetzgebungsvorschlag in vollem Einklang stehen muss insbesondere mit dem derzeitigen EU-Datenschutzrechtsrahmen sowie mit dem EU-Recht und der Rechtsprechung im Allgemeinen“ (keine offizielle Übersetzung).[16] In der „Erklärung zu elektronischen Beweismitteln“ (keine offizielle deutsche Übersetzung) verweist die Arbeitsgruppe insbesondere auf Artikel 48 der Datenschutz-Grundverordnung der Europäischen Union, der Regelungen enthält zu bestimmten grenzüberschreitenden „nach dem Unionsrecht nicht zulässige[n] Übermittlungen oder Offenlegungen“.[17] Der Artikel sieht vor, dass jegliches Urteil eines Gerichts eines Drittlands oder jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands „mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird“, unbeschadet anderer Gründe für die Übermittlung gemäß Kapitel V „jedenfalls nur dann anerkannt oder vollstreckbar werden“ dürfen, „wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind“. In diesem Zusammenhang erinnert die Art. 29-Datenschutzgruppe daran, dass das EU-Datenschutzrecht vorsieht, dass bestehende internationale Abkommen, wie ein Rechtshilfeabkommen (MLAT), in der Regel eingehalten werden müssen, wenn Strafverfolgungsbehörden in Drittstaaten den Zugang oder die Offenlegung von den für die Verarbeitung Verantwortlichen in der EU verlangen.[18] Im Namen der Europäischen Union kam die Europäische Kommission in ihrem „Amicus brief“ im Fall USA gegen Microsoft zu dem Schluss, dass die Datenschutz-Grundverordnung die MLATs zur "bevorzugten Option für Datentransfers" macht, wobei sie feststellt, dass eine Übermittlung durchgeführt werden kann, wenn andere Rechtsgründe für einen Datentransfer vorliegen.[19] Daran anschließend erörtert die EU-Kommission im „brief“ die Anwendbarkeit der Ausnahmeregelungen für das öffentliche Interesse und die berechtigten Interessen des für die Verarbeitung Verantwortlichen im konkreten Fall.[20]

In den USA wurde im März 2018 der "CLOUD Act" in Kraft gesetzt.[21] Das Gesetz ändert das US-Recht dahingehend, dass die Strafverfolgungsbehörden die Offenlegung von Daten, die außerhalb der USA gespeichert sind, erzwingen können (vorbehaltlich der Anfechtung durch Dienstanbieter).[22] Der CLOUD Act ermächtigt die Exekutive auch dazu, Vereinbarungen über den direkten Zugriff aus-

---

ments und des Rates zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren“ (https: //eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM: 2018: 226: FIN) vorgeschlagen. Weiteres *siehe* unter Pressemitteilung der EU-Kommission, *Sicherheitsunion: Kommission erleichtert den Zugang zu elektronischen Beweismitteln* (Apr. 17, 2018), http: //europa.eu/rapid/press-release_IP-18-3343_en.htm.

[15] Pressemitteilung der Artikel 29-Arbeitsgruppe zur Plenarsitzung vom November 2017 (Dezember 5, 2017), http: //ec.europa.eu/newsroom/just/document.cfm?doc_id=48748.

[16] *Ebenda*

[17] Erklärung der Artikel 29-Datenschutzgruppe, *Data protection and privacy aspects of cross-border access to electronic evidence*, (Nov. 29, 2017), http: //ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610177.

[18] Ebenda

[19] EU-Kommission, *Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party*, United States v. Microsoft, No. 17-2 (Dec. 13, 2017), https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf.

[20] *Ebenda*

[21] Consolidated Appropriations Act, 2018, div. V, Pub. L. No.115-141(2018).

[22] § 103.

ländischer Regierungen auf in den USA gespeicherte Daten zu treffen, wenn Bundesbeamte bestätigen, dass die jeweilige Regierung die Privatsphäre und die bürgerlichen Freiheiten ausreichend schützt; eine Entscheidung, die vor Gericht nicht überprüft werden kann.[23]

Bemerkungen und Empfehlungen der IWGDPT

Da immer mehr Daten die Grenzen überschreiten, müssen die derzeitigen und künftigen rechtlichen Rahmenbedingungen trotz unterschiedlicher nationaler Rechtssysteme strenge Datenschutzstandards einhalten. Zunehmende grenzüberschreitende Forderungen nach Daten bei der Strafverfolgung werden insbesondere dann neue Herausforderungen mit sich bringen, wenn das ersuchende Land den Zugriff auf personenbezogene Daten, das Kopieren, das Abfangen oder andere Eingriffe im Zusammenhang mit personenbezogenen Daten unterhalb anerkannter Datenschutznormen gestattet.

Die Mechanismen zur Erleichterung des strafrechtlichen grenzüberschreitenden Zugriffs auf Daten sollten die Interessen des Datenschutzes und der Privatsphäre wahren und gleichzeitig die rasche und angemessene Bearbeitung legitimer grenzüberschreitender Datenanfragen fördern.

Unter Hinweis darauf, **dass**

- auf der 51. Sitzung der IWGDPT in Polen die Empfehlung ausgesprochen wurde, dass das Cloud-Computing im Vergleich zu herkömmlichen Datenverarbeitungen nicht zu einer Absenkung der Datenschutzstandards führen darf[24]

- auf der 54. Sitzung der IWGDPT in Berlin die Regierungen dringend aufgefordert wurden, die Bürgerinnen und Bürgern zu ermächtigen und diese zu ermutigen, dass sie frei Werkzeuge zur sicheren Kommunikation erforschen, schaffen, verbreiten und nutzen[25]

- auf der 57. Sitzung der IWGDPT in Seoul die Regierungen aufgefordert wurden, dass Behörden verpflichtet werden, eine obligatorische statistische Berichterstattung über die Nutzung von Befugnissen für den Zugriff zu den von Unternehmen gehaltenen personenbezogenen Daten vorzusehen[26]

in Bekräftigung der Bedeutung von völkerrechtlichen Instrumenten, die den Schutz der Privatsphäre als Grundrecht vorsehen, insbesondere

- Artikel 12 der „Allgemeinen Erklärung der Menschenrechte“, in dem es heißt: „Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen“

---

[23] § 105.

[24] Arbeitspapier zum Cloud-Computing – Datenschutz- und Datenschutzfragen – „Sopot Memorandum“, angenommen auf der 51. Sitzung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation am 23./24. April 2012 in Sopot (Polen), https: //www.datenschutz-berlin.de/working-paper.html.

[25] Arbeitspapier zum Recht auf vertrauliche Telekommunikation, angenommen auf der 54. Sitzung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation am 2./3. September 2013 in Berlin (Deutschland), https: //www.datenschutz-berlin.de/working-paper.html.

[26] Arbeitspapier zu Transparenzberichten: Förderung der Rechenschaftspflicht staatlicher Stellen beim Zugriff auf personenbezogene Daten, die sich im Besitz von Unternehmen befinden, angenommen auf der 57. Sitzung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation am 27./28. April 2015 in Seoul (Korea), https: //www.datenschutz-berlin.de/working-paper.html.

- Artikel 17 des „Internationalen Pakt über bürgerliche und politische Rechte“, in dem es heißt, [hinsichtlich aller im Gebiet der Vertragspartei befindlichen und seiner Herrschaftsgewalt unterstehenden Personen] „(1) Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden“ und „(2) Jedermann hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen“

- Artikel 8 der „Europäischen Menschenrechtskonvention“, in dem es heißt es, „(1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz“ und „(2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer“

- Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union, in denen es heißt, „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation“ und „(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht“

unter Betonung der Garantien eines wirksamen Rechtsbehelfs bei einer Rechtsverletzung, einer fairen Anhörung vor einem unparteiischen Gericht und der Rechtmäßigkeit gemäß den Artikeln 8 bis 11 der Allgemeinen Erklärung der Menschenrechte, den Artikeln 2, 14 und 15 des Internationalen Pakts über bürgerliche und politische Rechte, den Artikeln 6, 7 und 13 der Europäischen Konvention zum Schutz der Menschenrechte und den Artikeln 47 und 49 der Charta der Grundrechte der Europäischen Union.

Die 62. Sitzung der Internationalen Arbeitsgruppe **erkennt** die Risiken für die Privatsphäre und die Datenschutzrechte einer Person **an**, wenn ausländische Datenanfragen den Schutz im nationalen oder internationalen Recht umgehen können. Die Arbeitsgruppe **stellt ferner fest**, dass grenzüberschreitende Datenanfragen, die auf einem klaren Rechtsverfahren beruhen, wichtigen nationalen Strafverfolgungsbedürfnissen dienen.

Empfehlungen

Die Arbeitsgruppe empfiehlt, dass Regierungen und internationale Organisationen daran arbeiten sicherzustellen, dass grenzüberschreitende Datenanfragen zur Strafverfolgung mit den internationalen Menschenrechtsnormen für die Rechtspflege in Einklang stehen und dass die Mechanismen zur grenzüberschreitenden Datenübermittlung im Rahmen der Strafverfolgung, sei es im Wege eines MLAT oder jeglichen anderen Mechanismus, so konzipiert sind, dass angemessene Datenschutzgarantien und der Schutz der Privatsphäre und des Schriftverkehrs gewährleistet sind:

- **Rechenschaftspflicht.** Die Transfermechanismen sollten gewährleisten, dass alle an dem Verfahren beteiligten Akteure für ihre Maßnahmen angemessen rechenschaftspflichtig sind.

- **Prozessuale Fairness** ("due process"). Die Transfermechanismen sollten sicherstellen, dass den betroffenen Personen ihr Recht auf ein faires Verfahren (rechtstaatliches Verfahren) garantiert ist, welches klare und transparente rechtliche Standards und Verfahren für Anträge einschließt.

- **Wirksamkeit.** Die Wirksamkeit starker Transfermechanismen sollte im Vordergrund stehen, um eine zügige und regelmäßige Bearbeitung von Ersuchen zu erleichtern, unter anderem durch die Festlegung gegenseitig verständlicher Auslegungen von Rechtsnormen und von Verfahren für die Ersuchen sowie die Bereitstellung ausreichender Ressourcen für die Transfermechanismen.

- **Bekanntmachung und Anfechtungsmöglichkeit.** Die betroffenen Personen sollten das Recht haben, benachrichtigt zu werden, und die Möglichkeit haben, das Ersuchen eines ausländischen Staates auf Zugriff auf ihre personenbezogenen Daten anzufechten.

- **Erforderliche und angemessene Festlegungen.** Niemand sollte einem geringeren Standard für ein rechtliches Verfahren unterworfen werden, als es geltende internationale Menschenrechtsnormen und Rechtsrahmen für den Schutz der Privatsphäre und personenbezogener Daten vorsehen, einschließlich der Erforderlichkeit für legitime Zwecke und der Verhältnismäßigkeit.

- **Richterliche Genehmigung.** Ersuchen sollten der gerichtlichen Genehmigung und Überprüfung unterliegen.

- **Aufsicht.** Es sollte eine angemessene unabhängige Kontrolle über die Transfermechanismen geben.

- **Transparenzmechanismus.** Eine formelle öffentliche Berichterstattung über die Ersuchen in Form von aggregierten Statistiken sollte vorgeschrieben sein.[27]

[27] Arbeitspapier zu Transparenzberichten: Förderung der Rechenschaftspflicht staatlicher Stellen beim Zugriff auf personenbezogene Daten, die sich im Besitz von Unternehmen befinden, angenommen auf der 57. Sitzung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation am 27./28. April 2015 in Seoul (Korea), https: //www.datenschutz-berlin.de/working-paper.html.