



43. Geschlossene Sitzung des Global Privacy Assembly

Oktober 2021

Angenommene Entschließung zum Zugang der Regierungen zu Daten, zum Datenschutz und zur Rechtsstaatlichkeit: Grundsätze für den Zugang der Regierungen zu personenbezogenen Daten des privaten Sektors zu Zwecken der nationalen Sicherheit sowie der öffentlichen Sicherheit

SPONSOREN:

- Commission Nationale de l'Informatique et des Libertés (CNIL – Frankreich)
- Personal Information Protection Commission (PPC – Japan)
- Office of the Privacy Commissioner of Canada (OPC – Kanada)

CO-SPONSOREN:

- Office of the Privacy Commissioner, Te Mana Matapono Matatapu (Neuseeland)
- Europäischer Datenschutzbeauftragter (Europäische Union)
- Data Protection Commissioner (Malta)
- Autorità Garante per la protezione dei dati personali (San Marino)
- Autorité de protection des données – Gegevensbeschermingsautoriteit (Belgien)
- Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) (Schweiz)
- Information and Privacy Commissioner of Ontario (Kanada)
- Commission Nationale pour la Protection des Données (Luxemburg)
- National Privacy Commission (Philippinen)
- Europäischer Datenschutzbeauftragter (Europarat)
- Comissão Nacional de Protecção de Dados (Portugal)
- Datenschutzkommission (Österreich)

- Information Commissioner’s Office (ICO – Vereinigtes Königreich)
- Instance nationale de protection des données à caractère personnel (INPDP – Tunesien)
- Personal Information Protection Commission (PIPC – Republik Korea)
- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI – Deutschland)

Die 43. jährliche geschlossene Sitzung des Global Privacy Assembly

Unter Hinweis auf die EntschlieÙung der ICDPPC zur strategischen Ausrichtung der Konferenz (2019-21)¹

Unter Hinweis auf die EntschlieÙung der ICDPPC über das Recht auf Privatsphäre als grundlegendes Menschenrecht und als Voraussetzung für die Wahrnehmung anderer Grundrechte ²

Unter Hinweis auf die EntschlieÙung der ICDPPC zur transparenten Berichterstattung³

Unter Hinweis auf das im April 2017 angenommene Arbeitspapier der Internationalen Arbeitsgruppe für den Datenschutz in der Telekommunikation zu internationalen Grundsätzen oder Instrumenten zur Regulierung der nachrichtendienstlichen Informationsbeschaffung ⁴

Unter Hinweis auf die EntschlieÙung der AFAPDP vom November 2013, die auf mehr Transparenz bei der Erhebung personenbezogener Daten durch die Regierungen abzielt;⁵

Unter Hinweis auf das Communiqué des Runden Tisches der G7- Datenschutzbehörden vom 7./8. September 2021 zum Thema „Freier Datenverkehr mit Vertrauen“⁶

Unter Hinweis darauf, dass die Achtung der Rechtsstaatlichkeit, der demokratischen Werte und der Menschenrechte im Mittelpunkt der Datenschutzregelungen und der Datenschutzgesetze steht,

In der Erwägung, dass die Grundsätze des Schutzes der Daten und der Privatsphäre in Bezug auf den Zugang der Regierungen zu personenbezogenen Daten und sensiblen Informationen wesentliche Elemente sind, die die Achtung der Rechtsstaatlichkeit, der demokratischen Werte und der Menschenrechte im Hinblick auf das legitime Ziel der Wahrung der nationalen und öffentlichen

¹ <https://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-the-Conference-Strategic-Direction-2019-2021-FINAL.pdf>

² <https://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-privacy-as-a-fundamental-human-rechts-2019-FINAL-DE.pdf>

³ <https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Transparency-Reporting.pdf>

⁴ <https://www.datenschutz-berlin.de/infotehke-und-service/veroeffentlichungen/working-paper>

⁵ <https://www.afapdp.org/archives/download-view/2013-resolution-sur-la-transparence>

⁶ <https://ico.org.uk/media/about-the-ico/documents/4018242/g7-attachment-202109.pdf>

Sicherheit gewährleisten,

In der Erwägung, dass die Bedeutung dieser Schlüsselemente in der Rechtsprechung hoher Gerichte in mehreren Teilen der Welt unterstrichen wurde,

In der Erkenntnis, dass Regierungsbehörden, die den Zugang zu den im privaten Sektor gespeicherten personenbezogenen Daten und sensiblen personenbezogenen Daten beantragen, ein legitimes Ziel der öffentlichen Ordnung verfolgen und zur Wahrung der Freiheit und Sicherheit beitragen, und dass Datenschutzgarantien dazu beitragen, die Rechtmäßigkeit, Legitimität und Rechenschaftspflicht nationaler Sicherheitsmaßnahmen und Programme für die öffentliche Sicherheit zu verbessern,

Unter Hinweis darauf, dass die Entwicklung einer datengesteuerten Wirtschaft, die sich zunehmend auf die Verarbeitung personenbezogener Daten stützt, ein ständig wachsendes Volumen an personenbezogenen, bei Unternehmen des privaten Sektors vorliegenden Daten und sensiblen Informationen auf internationaler Ebene mit sich bringt. Diese Daten sind eine wesentliche Informationsquelle für Regierungen und Behörden zur Verfolgung wichtiger Ziele im öffentlichen Interesse,

In Anerkennung, dass Transparenz, einschließlich sowohl der Information der Öffentlichkeit als auch der Bereitstellung von Informationen für einzelne betroffene Personen, vorbehaltlich der erforderlichen und verhältnismäßigen Beschränkungen, ein wesentliches Element der Rechenschaftspflicht der Regierungen und der Fähigkeit der Bürger ist, ihre Rechte in einer demokratischen Gesellschaft wahrzunehmen,

Unter Hinweis darauf, wie wichtig es ist, die Vertraulichkeit elektronischer Kommunikationssysteme und damit zusammenhängender Sicherheitsmerkmale wie kryptografische Systeme zu wahren, und **unter besonderem Hinweis** auf Berichte darüber, dass seitens gewisser staatlicher Stellen eine angebliche Nutzung besonders tief in die Privatsphäre eindringender Technologien erfolgte, die von privaten Dienstleistern bereitgestellt wurden,

Unter der Betonung, dass hohe Gewährleistungen für den Schutz der Daten und der Privatsphäre von entscheidender Bedeutung für die Wahrung des Vertrauens der Öffentlichkeit, die Förderung der Marktinteroperabilität und die Unterstützung des internationalen Austauschs personenbezogener Daten und des grenzüberschreitenden Datenflusses sind,

Darauf verweisend, dass neben den Risiken für die Privatsphäre als grundlegendes Menschenrecht und für andere Grundrechte auch das Fehlen ausreichender Garantien für den Schutz der Daten und

der Privatsphäre in Bezug auf den Zugang der Regierungen zu personenbezogenen, im Privatsektor gespeicherten Daten, schwerwiegende Herausforderungen für den freien Verkehr personenbezogener Daten auf internationaler Ebene darstellt und eine Hürde für die globale digitale Wirtschaft sein kann,

In der Erkenntnis, dass unterschiedliche Rechtssysteme und -traditionen auf regionaler und internationaler Ebene koexistieren und dass die Konvergenz in Richtung auf die wichtigsten Grundsätzen und hohen Standards für den Zugang der Regierungen zu personenbezogenen Daten des Privatsektors zur Rechtssicherheit und zur Erleichterung des Datenflusses in der globalen digitalen Wirtschaft beitragen kann,

Unter Berücksichtigung der wichtigen laufenden internationalen Initiativen und Diskussionen in verschiedenen Foren (z. B. Europarat, OECD, G20/G7, Vereinten Nationen) sowie der bilateralen Verhandlungen und Vereinbarungen über den Zugang der Regierungen zu personenbezogenen Daten des Privatsektors zu Zwecken der nationalen sowie der öffentlichen Sicherheit,

Unter Hinweis auf das Ziel des Global Privacy Assembly, seine Rolle und seine Stimme in einer breiteren Debatte über die digitale Politik auf internationaler Ebene zur Förderung hoher Standards zu stärken **und unter Betonung der Notwendigkeit**, die durchgängige Wahrung des Schutzes der Daten und der Privatsphäre in den laufenden Entwicklungen zu gewährleisten, die sich auf die digitale Wirtschaft auf internationaler Ebene auswirken,

verabschiedet das Global Privacy Assembly daher die folgende EntschlieÙung zum Zugang der Regierungen zu Daten, zum Datenschutz und zur Rechtsstaatlichkeit und spricht sich dafür aus, die folgenden Grundsätze für den Zugang der Regierungen zu personenbezogenen Daten des Privatsektors zu Zwecken der nationalen sowie der öffentlichen Sicherheit anzuwenden, wodurch Bedingungen zur Gewährleistung festgelegt werden, dass jede Art des rechtmäßigen Zugangs der Behörden zu Zwecken der nationalen oder der öffentlichen Sicherheit auch zur Wahrung der Privatsphäre und der Rechtsstaatlichkeit beiträgt:

1. **Rechtsgrundlage:** Der Zugang der Regierungen zu personenbezogenen Daten muss nach öffentlicher Debatte und Prüfung durch die Gesetzgeber durch angemessene, erlassene Rechtsvorschriften ordnungsgemäß genehmigt werden. Die Rechtsvorschriften müssen das Recht auf den Schutz der Daten und der Privatsphäre sowie andere Menschenrechte achten und dürfen nicht diskriminierend sein.

2. Klare und präzise Rechtsvorschriften für den Zugang der Regierungen:

Rechtsvorschriften, die den Zugang zu personenbezogenen Daten gestatten, sollten

- a) öffentlich zugänglich sein,
- b) in klarer, leicht verständlicher Sprache **abgefasst** sein und,
- c) präzise und spezifisch hinsichtlich des Umfangs personenbezogener Daten sein, für die das Gesetz Zugang für staatliche Stellen gewährt, und hinsichtlich der Bedingungen für diesen Zugang.

3. Allgemeiner Grundsatz der Notwendigkeit und Verhältnismäßigkeit: Damit der Zugang zu personenbezogenen Daten, einschließlich sensibler Daten, durch staatliche Behörden oder staatliche Stellen gerechtfertigt sein kann, muss die spezifische Verwendung für personenbezogene Daten mit einer nachweislich notwendigen Funktion oder Tätigkeit der Regierungen verknüpft werden, und der Grad des Eingriffs in die Privatsphäre muss in einem angemessenen Verhältnis zum jeweiligen Ziel stehen.

4. Transparenz: Alle Vereinbarungen oder Abkommen über den Zugang der Regierungen, die sich aus einer gesetzlichen Genehmigung ergeben, sollten auch proaktive, grundlegende öffentliche Berichterstattungspflichten und öffentlich zugängliche Rechenschaftsverfahren für die beteiligten staatlichen Stellen vorsehen und das Informieren der betroffenen Personen ermöglichen, es sei denn, Beschränkungen der Transparenz gegenüber Einzelpersonen stellen eine notwendige und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft dar.

5. Rechte der betroffenen Person: Unter Berücksichtigung der Anforderungen für die nationale sowie für die öffentliche Sicherheit sollte der Zugang der Regierungen zu personenbezogenen Daten einen konkreten und spezifischen Rahmen für die Ausübung der Rechte durch Einzelpersonen beinhalten. Dazu gehört unter anderem auch, dass die Einzelpersonen ihre Anfragen direkt an Behörden richten können. Insbesondere sollten Einzelpersonen das Recht auf Auskunft und Berichtigung oder Löschung personenbezogener Daten haben, es sei denn, Beschränkungen der Rechte betroffener Personen stellen eine notwendige und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft dar.

6. Unabhängige Aufsicht: In Bezug auf Gesetze, die den Zugang gestatten, sollten sowohl eine unabhängige Aufsicht im Vorfeld (z. B. vorherige gerichtliche Genehmigung) als auch eine nachträgliche Überprüfung (z. B. Prüfung der Verarbeitung durch eine unabhängige

Regulierungsstelle) in Erwägung gezogen werden, wobei die Bedenklichkeit und Schwere der Auswirkungen der durch den konkreten Zugang der Regierungen verursachten Auswirkungen auf die Grundrechte und Grundfreiheiten von Einzelpersonen zu berücksichtigen sind.

7. Gesetzliche Beschränkung der Nutzung der erlangten Daten durch staatliche Stellen:

Rechtsvorschriften, die den Zugang der Regierungen zu personenbezogenen Daten für einen bestimmten Zweck gestatten, sollten Regelungen und Beschränkungen für alle sekundären Verwendungen oder Weiterübermittlungen für andere Zwecke festlegen, wobei auch allgemeine Grundsätze zur Gewährleistung eines kontinuierlichen Schutzes personenbezogener Daten zu beachten sind.

8. Wirksame Rechtsmittel und Rechtsbehelfe, die den Betroffenen zur Verfügung stehen:

Jeder staatliche Zugang zu personenbezogenen Daten sollte besonderen Bestimmungen unterliegen, damit betroffene Personen wirksame Rechtsmittel und Rechtsbehelfe in Anspruch nehmen können.

Ergänzend zu den oben genannten Grundsätzen **betrachtet das Global Privacy Assembly die folgenden Beispiele und bewährten Verfahren als relevante Beispiele für die weitere Rechenschaftspflicht beim Zugang der Regierungen zu personenbezogenen Daten und für die Umsetzung wichtiger Garantien** zur Gewährleistung des Schutzes der Privatsphäre und der personenbezogenen Daten natürlicher Personen:

- **Die Gewährleistung, dass kryptografische Systeme nicht durch Zugangsanforderungen für staatliche Stellen untergraben werden, was einen ausnahmsweise gewährten Zugang** durch die bewusste Einführung von Schwachstellen im Bereich der Cybersicherheit (z. B. vorgeschriebene „Backdoors“) mit sich bringen könnte.
- Unternehmen sollen **transparente Berichte vorlegen**, in denen die Zahl der Anfragen durch staatliche Stellen dokumentiert wird;
- **Zusätzliche Möglichkeiten** für Rechtsmittel und Rechtsbehelfe des Privatsektors in Bezug auf den Zugang der Regierungen zu personenbezogenen Daten, um die Anwendung des oben genannten Grundsatzes der wirksamen Rechtsmittel und Rechtsbehelfe zu unterstützen und zu erleichtern;
- **Internationale regulatorische Zusammenarbeit** bei der Aufsicht und Überwachung des Zugangs der staatlichen Stellen zu personenbezogenen Daten.

Das Global Privacy Assembly entschließt sich zur Unterstützung und Verteidigung der oben

genannten Grundsätze und bewährten Verfahren in Bezug auf den Zugang der Regierungen zu personenbezogenen, im Privatsektor vorliegenden Daten zu Zwecken der nationalen sowie der öffentlichen Sicherheit.

Das Global Privacy Assembly fordert die Regierungen und internationalen Organisationen auf, die oben genannten Grundsätze zu beachten und auf die Entwicklung multilateraler Instrumente hinzuarbeiten, mit denen die Einhaltung der wichtigsten Grundsätze des Schutzes der Daten und der Privatsphäre in Bezug auf den Zugang der Regierungen zu personenbezogenen Daten gewährleistet wird.

Im Einklang mit den oben genannten Grundsätzen fordert das Global Privacy Assembly auch Regierungen und internationale Organisationen auf, Gespräche zu führen, die darauf abzielen, den Verkauf, den Export und die Nutzung von Technologien zu regeln, die einen besonders in die Privatsphäre eingreifenden und unverhältnismäßigen Zugang zu personenbezogenen Daten, insbesondere zu elektronischen Kommunikationsinhalten und -daten, ermöglichen.

Die U.S. Federal Trade Commission und das Büro des Datenschutzbeauftragten für personenbezogene Daten, Hongkong, China enthalten sich von dieser EntschlieÙung, die sich auf Angelegenheiten auÙerhalb ihrer jeweiligen Gerichtsbarkeit bezieht.