DIGITALE GESELLSCHAFT.DE

Digitale Gesellschaft e.V.
Singerstraße 109
10179 Berlin

+49 30 97894230

info@digitalegesellschaft.de
www.digitalegesellschaft.de
@digiges

Berlin, den 20.04.17

# Stellungnahme des Digitale Gesellschaft e.V. zum Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681

# (Fluggastdatengesetz – FlugDaG)

Zu dem vorliegenden Entwurf nehmen wir wie folgt Stellung:

## Vorbemerkung:

Als Reaktion auf terroristische Anschläge und organisierte, grenzüberschreitende Kriminalität wurde die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität auf den Weg gebracht.

Ziel ist es, durch die Einführung einer Vorratsdatenspeicherung von Fluggastdaten, nicht nur bekannte, sondern auch „bisher unbekannte Verdächtige“[1] zu identifizieren. Hierfür wird eine Fluggastdatenzentralstelle die von den Luftfahrtunternehmen übermittelten PNR-Daten mit bestehenden Datenbeständen und Mustern abgleichen. Jene Muster werden auch aus den zuvor übermittelten PNR-Daten erstellt und aktualisiert. Sowohl die PNR-Daten als auch die Ergebnisse der Verarbeitung dieser Daten können an das Bundeskriminalamt, die Landeskriminalämter, die Zollverwaltung, die Bundespolizei, das Bundesamt für Verfassungsschutz sowie die Verfassungsschutzbehörden der Länder, den Militärischen Abschirmdienst und den Bundesnachrichtendienst weitergeleitet werden. Zudem können die PNR-Daten als auch die Ergebnisse an andere Mitgliedstaaten der Europäischen Union, Europol sowie Drittstaaten übermittelt werden.

Die Speicherung und Auswertung von PNR-Daten erfolgt mittlerweile in einigen Staaten. Nationale PNR-Systeme gibt es etwa in Großbritannien, Schweden und Frankreich. Zudem bestehen Abkommen zur Übermittlung von Fluggastdaten zwischen der EU und den USA sowie Australien. Obwohl diese Staaten seit mehreren Jahren PNR-Daten im Kampf gegen Terrorismus und organisierte Kriminalität nutzen, gibt es keinen konkreten Nachweis dafür, dass eine Fluggastdatenspeicherung für die Bekämpfung von organisierter Kriminalität und Terrorismus ein taugliches Mittel wäre. Zugleich ist der Eingriff in die Grundrechte der Reisenden massiv: Die PNR-Daten von allen Reisenden auf Flügen, die zwischen den Mitgliedstaaten der EU durchgeführt werden als auch die von einem Mitgliedstaat der Europäischen Union aus in einen Drittstaat oder von einem Drittstaat aus in einen Mitgliedstaat der Europäischen Union starten, werden für fünf Jahre auf Vorrat gespeichert und verarbeitet, ohne das ein konkreter Tatverdacht vorliegt. Die PNR-Daten berühren zudem in ihrer Gesamtheit den Bereich des Privatlebens und lassen Rückschlüsse auf das Intimleben der Reisenden zu. Die Speicherung und Verarbeitung von PNR-Daten widerspricht damit Europäischen Grundrechten (Art. 7 und Art. 8 Charta).

# Im Einzelnen:

## Datenübermittlung

Zunächst ist anzumerken, dass im Entwurf des FlugDaG vorgesehen ist, dass die Fluggastdaten für alle Flüge, die von der Bundesrepublik Deutschland aus starten und

1 KOM(2011) 32 endgültig, S.4

in einem anderen Staat landen oder von einem anderen Staat aus starten und in der Bundesrepublik Deutschland landen oder zwischenlanden, gespeichert und ausgewertet werden. Die Anwendung der Richtlinie auf innereuropäische Flüge ist in der Richtlinie nicht verpflichtend vorgeschrieben. Das Ausdehnen der Richtlinie auf innereuropäische Flüge wird in der Begründung des Gesetzes damit erklärt, dass Täter und Tätergruppierungen im Bereich schwere Kriminalität und internationalem Terrorismus häufig Reiserouten innerhalb der Europäischen Union nutzen würden. Inwieweit Flugreisen dabei eine Rolle spielen und inwieweit die Erhebung und Auswertung von PNR-Daten nützlich sein kann, bleibt jedoch offen. Seitens der Europäischen Institutionen wird die Auswertung von Reisedaten innereuropäischer Flüge als nicht notwendig betrachtet, da diese nicht vorgeschrieben ist. Die lapidare Begründung, dass die angesprochenen Täter und Tätergruppierungen innereuropäische Reiserouten nutzen, erfüllt die Anforderungen an ein evidenzbasiertes Sicherheitskonzept nicht.

Unklar bleibt darüber hinaus, warum die in §2 (2) angeführten Daten, die durch die Luftfahrtunternehmen zu übermitteln sind, nötig sind, um den Zielen der Richtlinie gerecht zu werden. Die Daten berühren in ihrer Gesamtheit den Bereich des Privatlebens und lassen Rückschlüsse auf das Intimleben der Reisenden zu. Neben Informationen zu Kontaktdaten wie E-Mail-Adresse, Telefonnummer und Anschrift finden sich etwa auch Informationen über Mitreisende oder Zahlungsinformationen in den PNR-Daten. Unklar ist, welche Informationen in dem Datenfeld 16 „allgemeine Hinweise" gespeichert und verarbeitet werden. In diesem Freifeld können umfassende, darunter auch sensible Informationen, über die Reisenden gespeichert werden. Da es sich um ein Freifeld handelt, können diese Informationen auch nicht automatisiert gelöscht werden, sodass im Vorfeld der Speicherung und Auswertung der Daten sensible Informationen händisch gelöscht werden müssen. Die Erfahrungen[2] der australischen Behörden bei dem automatisierten Filtern und Löschen sensibler Daten in Bezug auf das Freifeld zeigen, dass hier ein enormer Arbeitsaufwand droht. Die Vorgaben aus §13 (3) FlugDaG dürften daher nur schwer zu erfüllen sein, zumindest fehlt jedoch ein Hinweis im Gesetz oder der Begründung, wie dieses Problem gelöst werden soll. Eine Begründung, warum diese Informationen notwendig sind und nicht etwa die

2 SWD(2014) 236 final, S.9

Auswertung und Speicherung von API-Daten ausreichend wäre, bleibt der Gesetzgeber schuldig. Ebenso bleibt unklar, wie die übermittelten Daten verifiziert werden können. Luftfahrtunternehmen sammeln und speichern PNR-Daten, um den reibungslosen Ablauf der Reise gewährleisten zu können. Neben verschiedenen internen Fehlerquellen, die zu falschen Angaben in einem PNR-Datensatz führen können, besteht zudem die Möglichkeit, durch Angriffe auf das System oder Hacks die Daten zu manipulieren und zu verfälschen. Sollten dabei Fehler auftreten, ist dies zwar ärgerlich für die Reisenden, jedoch drohen keine ernsthaften Konsequenzen. Wenn jedoch ein PNR-Datensatz mit falschen Informationen den Ermittlungsbehörden zur Verfügung gestellt wird, können daraus massive Einschnitte in die Grundrechte für die Betroffenen resultieren.

## Datenverarbeitung

Die Fluggastdatenzentralstelle kann die Fluggastdaten automatisch mit Datenbeständen, die der Fahndung oder Ausschreibung von Personen oder Sachen dient, abgleichen. Hinzu kommt der Abgleich mit Mustern. Jene Muster werden von der Fluggastdatenzentrale aus den zuvor übermittelten Fluggastdaten selbst erstellt. Durch diese Profiling-Maßnahme sollen verdachtsbegründende und verdachtsentlastende Prüfungsmerkmale so miteinander kombiniert werden, „dass die Zahl der unter ein Muster fallenden Personen möglichst gering ist". Schon durch diese Formulierung wird ein massives Problem offensichtlich: Unbescholtene Bürgerinnen und Bürger können durch diese Profiling-Maßnahme in das Visier von Ermittlungsbehörden geraten. Im Rahmen der CeBIT wurde das technische System vorgestellt, mit dem die Datenanalyse durchgeführt werden soll. Am Ende der Analyse sollen 0,07% der Datensätze an die Ermittlungsbehörden weitergeleitet werden. Pro Jahr ist demnach mit über 100.000 Datensätzen zu rechnen, die durch die Profiling-Maßnahme entstehen. Zwar ist vorgesehen, dass die Treffer, die aus dieser Maßnahme resultieren, durch die Fluggastdatenzentrale individuell überprüft werden, jedoch gehen damit weitere Überwachungsmaßnahmen und Eingriffe in die Grundrechte der Betroffenen einher. Auch an dieser Stelle findet sich keine Begründung, warum nicht mehr oder weniger Datensätze überprüft werden müssen. Die Maßnahme, als auch ihr Ausmaß, werden allein auf Anekdoten gestützt, wirken willkürlich und entbehren jeder fachlichen Begründung.

Ein Blick in andere Staaten zeigt zudem, dass durch die Analyse von Reisedaten mit dem Ziel der Bekämpfung von schwerer Kriminalität und Terrorismus auch immer

wieder unbescholtene Bürger massive Einschränkungen ihrer Grundrechte in Kauf nehmen müssen. Die No Fly List der USA verdeutlicht die Problematik: Senatoren, Journalisten, Künstler aber auch Kinder landen immer wieder auf diesen Listen und werden an ihrer Reisefreiheit gehindert und mit massiven Überwachungsmaßnahmen konfrontiert. Mit solchen „false postive alerts" ist bei jeder Profiling-Maßnahme, wie sie auch im FlugDaG vorgesehen ist, zu rechnen. Problematisch bei einer algorithmischen Auswertung der PNR-Daten ist zudem, dass die Muster selbst diskriminierend sind, da verdachtsbegründende und verdachtsentlastende Prüfungsmerkmale vorgegeben werden. Ebenso muss davon ausgegangen werden, dass Personen, die tatsächlich in Verbindung mit schweren Straftaten oder Terrorismus stehen, durch die Datenanalyse nicht gefunden werden können.

## Speicherdauer

Erst nach fünf Jahren werden die PNR-Daten gelöscht. In dieser Zeit können sie, teilweise mit Einschränkungen, vollständig abgerufen und ausgewertet werden. Zudem werden sie in dieser Zeit auch für die Erstellung der Muster genutzt. Unklar ist bis zum heutigen Tag warum die Speicherdauer auf fünf Jahre festgeschrieben wurde. Erneut fehlt jegliche Grundlage, die eine Speicherdauer von fünf Jahren rechtfertigen würde. Die Speicherdauer kann damit weder als verhältnismäßig noch als angemessen bezeichnet werden.

## Weitergabe

Die PNR-Daten als auch die gewonnenen Erkenntnisse können im Inland an das Bundeskriminalamt, die Landeskriminalämter, die Zollverwaltung, die Bundespolizei, das Bundesamt für Verfassungsschutz sowie die Verfassungsschutzbehörden der Länder, den Militärischen Abschirmdienst und den Bundesnachrichtendienst weitergeleitet werden. Zudem können die PNR-Daten als auch die Ergebnisse an andere Mitgliedstaaten der Europäischen Union, Europol sowie Drittstaaten übermittelt werden. Durch die Weitergabe der Daten ist es nahezu unmöglich zu überprüfen, wie die entgegennehmenden Behörden

und Einrichtungen im folgenden mit den Daten umgehen und inwiefern sich diese an die Vorgaben aus dem FlugDaG halten. Es droht ein unübersichtliches und unkontrollierbares Netz von Datensilos zu entstehen.

### Missbrauchspotential

Über 170 Millionen Passagiere reisen jährlich in Deutschland im Luftverkehr, Tendenz steigend. Die Daten von all jenen Passagieren werden für fünf Jahre in einer Datenbank gespeichert und mit anderen Behörden und Einrichtungen weltweit geteilt, auf die eine unbestimmte Anzahl von Personen Zugriff hat. Auch hier zeigt ein Blick auf das EU-USA Fluggastdatenabkommen, dass der Kreis der Zugriffsberechtigten schnell unüberschaubar werden kann. Über 14.000 DHS-Officers haben dort Zugriff auf die Datensätze.[3] Allein die Datensätze, die in der Bundesrepublik Deutschland zu speichern sind, werden in kürzester Zeit die Milliardengrenze sprengen. Zwar soll ein „modernes Zugriffs- und Berechtigungsmanagement" vor Missbrauch sowie ein „angemessenes Datensicherheitsniveau" vor unbefugten Zugriffen schützen, jedoch dürfte die Datensammlung große Begehrlichkeiten erwecken. Wer Zugriff auf die Daten hat, kann sich über das Intimleben von Millionen Reisenden informieren. Zudem können die Daten leicht für andere als im FlugDaG vorgeschriebene Anwendungsbereiche, wie etwa Wirtschaftsspionage, missbraucht werden.

## Fazit:

Das FlugDaG schreibt eine verdachtsunabhängige und anlasslose Vorratsdatenspeicherung von Reisedaten ohne Beweis für den Nutzen der Datensammlung vor. Ziel der geplanten Massenüberwachung des europäischen Reiseverkehrs ist vorgeblich die Bekämpfung von Terrorismus und schwerer Kriminalität. Bislang fehlt es aber an jeglichen konkreten Nachweisen dafür, dass eine Fluggastdatenspeicherung für diesen Zweck ein taugliches Mittel wäre. Ganz im Gegenteil konnten sich beispielsweise die Mordanschläge von Paris im Januar und November 2015 ereignen, obwohl Frankreich bereits seit 2006 über Überwachungsinstrumente wie die Vorratsdatenspeicherung von Kommunikations- und Fluggastdaten verfügt. Die Attentäter befanden sich sogar schon lange vor den Anschlägen fast allesamt auf dem Radar der Behörden und konnten trotzdem ungehindert kreuz und quer durch Europa und in den Nahen Osten reisen. Gerade angesichts dieser behördlichen Versäumnisse leuchtet es nicht ein, die bereits

3 SWD(2017) 14 final, S.13

vorhandenen Datenberge weiter zu vergrößern und die Suche nach der Nadel im Heuhaufen damit noch schwieriger zu gestalten. Durch die Architektur des dezentralen Systems mit Passenger Information Units in jedem Mitgliedstaat der EU – in Deutschland in Form der Fluggastdatenzentralstelle – droht das bisherige Kommunikationsproblem zwischen den europäischen Ermittlungsbehörden weiter verschärft zu werden.

Mit der Richtlinie EU 2004/82 besteht bereits eine Maßnahme zur Übermittlung von Fluggastdaten. Eine Begründung, warum diese nicht ausreicht bzw. warum eine Reform dieser Richtlinie nicht geeigneter sein könnte, um die in dem FlugDaG genannten Ziele zu erreichen, bleibt der Gesetzgeber schuldig.

Zudem droht bereits jetzt die Ausweitung des Systems. Ein Blick nach Belgien zeigt, dass die heute zur Debatte stehende Fluggastdatenspeicherung schon morgen auch auf andere Verkehrsmittel ausgeweitet werden könnte. Es droht damit eine Total-Überwachung des Reiseverkehrs. Die Räume, in denen sich Menschen unbeobachtet vom Staat bewegen und entfalten können, werden zunehmend enger.

Die Urteile des Europäischen Gerichtshofs zur Vorratsdatenspeicherung von Kommunikationsdaten lassen zudem den Schluss zu, dass es sich bei dieser Maßnahme ebenfalls um eine grundrechtswidrige Überwachung handelt. Zur Zeit überprüft der EuGH zudem das EU-Kanada-PNR Abkommen. Die Entscheidung des EuGH sollte zumindest abgewartet werden, um nicht erneut Gesetze zu verabschieden, die die Grundrechte der Bürgerinnen und Bürger missachten.