Die 39. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre

Hongkong, 25.-29. September 2017

Entschließung über den Schutz personenbezogener Daten in automatisierten und vernetzten Fahrzeugen

Antragsteller:

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Deutschland)

Unterstützt von:

- **Commission de la Protection de la Vie Privée**
  die belgische Datenschutzbehörde
- **Commission Nationale de l'Informatique et des Libertés (CNIL)**
  die französische Datenschutzbehörde
- **Der Beauftragte für den Schutz personenbezogener Daten, Hong Kong, China**
- **Garante per la protezione dei dati**
  die italienische Datenschutzbehörde
- **Instituto Nacional de Acceso a la Información, Transparencia y Protección de Datos Personales (INAI)**
  Nationales Institut für Transparenz, den Zugang zu Informationen und den Schutz personenbezogener Daten, Mexiko
- **Office of the Privacy Commissioner, Neuseeland**
- **Informacijski pooblaščenec Republike Slovenije**
  die Informationsbeauftragte der Republik Slowenien
- **Préposé fédéral à la protection des données et à la transparence**
  Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)
- **Information Commissioner's Office, Vereinigtes Königreich**

In Anerkennung der Tatsache, dass automatisierte und vernetzte Fahrzeuge durch einen höheren Grad an Benutzerfreundlichkeit oder Komfort erhebliche Vorteile für die Nutzer bieten können, wie auch für die Allgemeinheit durch die Verbesserung der Verkehrseffizienz und der Verkehrssicherheit der Fahrer und ihrer Fahrgäste, der anderen Verkehrsteilnehmer und Fußgänger;

Unter der Betonung der raschen Fortschritte bei der Fahrzeugautomatisierung und der Technologien zur Vernetzung der Fahrzeuge, welche die Entwicklung und Einführung neuer und innovativer Produkte, Geräte oder Telematikdienste ermöglichen, die in vielen Fällen die Erhebung und Verarbeitung personenbezogener Daten aufgrund einer Vielzahl von eingebauten Sensoren mit einschließen, was angesichts der verschiedenen Szenarien, in denen Fahrzeuge von vielen Personen genutzt werden, neue Herausforderungen in Bezug auf das Recht auf den Schutz personenbezogener Daten und der Privatsphäre der Nutzer hervorruft;

In Anbetracht der Erklärung der G7-Verkehrsminister und des europäischen Kommissars für Verkehr auf ihrem Treffen in Cagliari, Italien, vom 21.-22 Juni 2017[1], die die Notwendigkeit der Einhaltung einschlägiger, bestehender Richtlinien über Cybersicherheit und Datenschutz anerkennt, und alle Akteure zu einer Bewertung auffordert, wie die notwendigen Daten zur Entwicklung von Dienstleistungen und Anwendungen zur Verbesserung der Sicherheit und der Verkehrsbedingungen unter gleichzeitiger Wahrung der Verbraucherinteressen hinsichtlich der Cybersicherheit und des Datenschutzes genutzt werden können;

Unter Kenntnisnahme der Erklärung der für die digitale Wirtschaft zuständigen G20- Minister auf ihrer Tagung in Düsseldorf, Deutschland, am 6. und 7. April 2017 über die Gestaltung der Digitalisierung für eine vernetzte Welt,[2] welche die Notwendigkeit zur Stärkung des Vertrauens in die digitale Wirtschaft durch die Einhaltung der rechtlichen Rahmenbedingungen für den Schutz der Privatsphäre und der Daten und durch die Erhöhung der Sicherheit bei der Nutzung der Informations- und Kommunikationstechnologie sowie die Notwendigkeit der Transparenz und des Verbraucherschutzes anerkennt;

Besorgt über den möglichen Mangel an verfügbaren Informationen, Auswahl- und Eingriffsmöglichkeiten sowie von wirksamen Mechanismen zur Einwilligung für Fahrzeughalter, Fahrer und ihre Mitfahrer, für die anderen Verkehrsteilnehmer und Fußgänger zur Kontrolle des Zugriffs auf die Fahrzeugdaten und fahrrelevanten Daten und deren Nutzung;

Unter Beobachtung der Entwicklung verschiedener Technologien für kooperative intelligente Verkehrssysteme, bei denen Fahrzeuge durch eine kontinuierliche Informationsübertragung

---

[1] http://www.g7italy.it/sites/default/files/documents/Final Declaration_0.pdf

[2] https://www.bmwi.de/Redaktion/DE/Downloads/G/g20-digital-economy-ministerial-declaration-english-version.pdf?__blob=publicationFile&v=12

an andere Fahrzeuge (V2V), an die Verkehrsinfrastruktur (V2i) oder an andere Einheiten von Dritten (V2X) ihre Positionsdaten und kinematische Daten austauschen, um einen Gesamtüberblick über die aktuelle Verkehrslage zur Erhöhung der Effizienz und Sicherheit im Straßenverkehr zu erhalten;

Besorgt darüber, dass die uneingeschränkte und wahllose Verbreitung der Daten durch die Fahrzeuge im Rahmen von V2V-, V2I- und V2X-Kommunikation zu unrechtmäßiger Nutzung, unbefugten Zugriffen auf die personenbezogenen Daten der Fahrer, der Fahrgäste oder der anderen Einzelpersonen, oder zur deren Weiterverarbeitung durch Dritte führen könnte;

Unter Hinweis darauf, dass andererseits Technologien für kooperative intelligente Verkehrssysteme so gestaltet werden müssen, dass die Rückverfolgbarkeit und die Authentifizierung von Fahrzeugen ermöglicht wird, unter der angemessenen Berücksichtigung der Grundsätze von Privacy by Design und Privacy by Default;

In Anerkennung der Tatsache, dass sich die Entwickler der verschiedenen Technologien für kooperative intelligente Verkehrssysteme über die aus solchen Technologien entstehenden Risiken für die Privatsphäre bewusst sind und erhebliche Anstrengungen zur Minimierung dieser Risiken durch die Verringerung der Menge von personenbezogenen Daten und durch die Erschwerung der Identifikation der Betroffenen unternommen haben,

Unter Hinweis darauf, dass eine umfassende Sammlung in einem Connected-Vehicles-System einschließlich eines kooperativen intelligenten Verkehrssystems verteilter Daten nicht nur zur Erstellung von Bewegungsprofilen führen könnte, sondern auch Unmengen an Daten zur Auswertung des Fahrverhaltens enthalten könnte, wodurch eine Sammlung dieser Daten wertvolle Informationen für bestimmte Stellen beinhalten könnte, wie z. B. für Kfz-Versicherungen, Fahrzeughersteller, Werbetreibende, Strafverfolgungsbehörden oder Behörden für die Verfolgung von Ordnungswidrigkeiten, besonders wenn diese z. B. mithilfe beliebiger von Fahrzeugen versendeter Identifikatoren personalisiert werden;

Unter der Erwähnung der bewährten Lösungen bei kostenpflichtigen Fernsehübertragungen und beim digitalen Polizeifunk zur Einschränkung des Zugriffs auf übermittelte Informationen auf berechtigte Empfänger;

Zur Kenntnis nehmend, dass die Beauftragten für den Datenschutz und für die Privatsphäre spezifische Leitlinien über Datenschutzbestimmungen herausgeben, die für Datenverarbeitungen oder technische Lösungen in Bezug auf automatisierte und vernetzte Fahrzeuge gelten;

Unter Kenntnisnahme der Tatsache, dass das Weltforum zur Harmonisierung fahrzeugtechnischer Vorschriften nunmehr Leitlinien für Cybersicherheit und Datenschutz in seine Gesamtresolution über Fahrzeugtechnik (R.E.3)[3] als Anhang 6 aufgenommen hat;

[3] https://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29resolutions/ECE-TRANS-WP.29-78r5e.pdf

Unter Bekräftigung der in Teil I Abschnitt 4 der oben-erwähnten Leitlinien über Cybersicherheit und Datenschutz festgelegten Anforderungen, die die Berücksichtigung der Konzepte bezüglich Privacy by Design und Privacy by Default beinhalten;

Unter erneuter Bekräftigung der Entschließung zu Privacy by Design[4], die von der 32. Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre 2010 in Jerusalem angenommen wurde, der Entschließung zu Profiling[5], die von der 35. Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre 2013 in Warschau angenommen wurde, sowie der Entschließung zu Big Data, die von der 36. Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre 2014 in Fort Balaclava, Mauritius[6], angenommen wurde;

Ruft die 39. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre alle beteiligten Parteien, insbesondere

- **Normungsgremien,**
- **Öffentliche Behörden,**
- **Fahrzeug- und Ausrüstungshersteller,**
- **Unternehmen für Privattransporte und Mietwagenanbieter,**
- **Anbieter von datengetriebenen Dienstleistungen, wie z. B. Spracherkennung, Navigation, Fernwartung oder Telematikdienste für KFZ-Versicherungen,**

dazu auf, die Grundrechte der Nutzer auf den Schutz ihrer personenbezogenen Daten und ihrer Privatsphäre in vollem Umfang zu achten und diesen Grundrechten in jeder Phase der Herstellung und Entwicklung neuer Geräte oder Dienstleistungen hinreichend Rechnung zu tragen.

Die oben genannten Parteien werden somit nachdrücklich aufgefordert,

1. die Betroffenen umfassend darüber zu informieren, welche Daten beim Einsatz von vernetzten Fahrzeugen zu welchem Zweck und durch wen gesammelt und verarbeitet werden,
2. Anonymisierungsverfahren zur Minimierung der Menge personenbezogener Daten zu nutzen, oder wenn dies nicht möglich ist, dann Pseudonymisierungsverfahren zu nutzen,

[4] https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf

[5] https://icdppc.org/wp-content/uploads/2015/02/Profiling-resolution2.pdf

[6] https://icdppc.org/wp-content/uploads/2015/2/Resolution-Big-Data.pdf

3. personenbezogene Daten nicht länger als notwendig für den rechtmäßigen Zweck, für den sie verarbeitet werden, für weitere vereinbare Zwecke oder gemäß den Rechtsvorschriften oder gemäß des Einverständnisses aufzubewahren und nach Ablauf dieses Zeitraums zu löschen.

4. technische Mittel zur Löschung personenbezogener Daten bereitzustellen, wenn ein Fahrzeug verkauft oder an seinen Eigentümer zurückgegeben wird,

5. granulare und leicht zu nutzende Auswahl- und Eingriffsmöglichkeiten für Fahrzeugnutzer bereitzustellen, die ihnen die Gewährung oder Ablehnung des Zugangs zu den verschiedenen Datenkategorien in Fahrzeugen ermöglichen,

6. technische Mittel für die Fahrzeugnutzer zur Einschränkung der Datensammlung bereitzustellen,

7. sichere Speichermedien bereitzustellen, die den Fahrzeugnutzern die vollständige Kontrolle über den Zugang zu den durch ihre Fahrzeuge erhobenen Daten erlauben,

8. technische Maßnahmen für Komponenten für eine sichere online Kommunikation bereitzustellen, die vor Cyberangriffen schützen und den unbefugten Zugang zu personenbezogenen Daten sowie deren Abfangen verhindern,

9. die Kommunikationstechnologien für kooperative intelligente Verkehrssysteme auf eine Weise zu entwickeln und umzustetzen, die

    a. den unbefugten Zugang zu personenbezogenen, von Fahrzeugen (V2V), Verkehrsinfrastrukturen (v2i) oder von anderen Einheiten von Dritten (v2x) gesammelten Daten sowie deren Abfangen verhindert,

    b. es den Fahrzeugnutzern erlaubt, den Austausch von Positionsdaten und kinematischen Daten zu unterbinden, aber weiterhin Gefahrenhinweise zu empfangen,

    c. Schutzmaßnahmen gegen eine unrechtmäßige Verfolgung und Ortung der Fahrer bietet,

    d. gewährleistet, dass durch die Sicherheitsmechanismen der V2V, V2i und V2x-Kommunikation zur Authentifizierung von Fahrzeugen keine zusätzlichen Risiken für den Schutz der Privatsphäre und der personenbezogenen Daten entstehen und

    e. das Risiko der Verfolgbarkeit und Identifizierbarkeit verringern.

10. die Grundsätze des Privacy by Default und des Privacy by Design zu wahren, indem sie technische und organisatorische Maßnahmen und Verfahren zur Verfügung stellen, die gewährleisten, dass die Privatsphäre der Betroffenen gewahrt ist,

sowohl bei der Festlegung der Mittel der Verarbeitung als auch bei der Datenverarbeitung,

11. Technologien und Architekturen zu entwickeln, die eine datenschutzfreundliche Verarbeitung personenbezogener Daten im Fahrzeug gewährleisten,

12. zu gewährleisten, dass selbstlernende Algorithmen für automatisierte und vernetzte Fahrzeuge in ihrer Funktionsweise transparent gemacht wurden und dass diese einer vorherigen Prüfung durch eine unabhängige Stelle unterzogen wurden, um das Risiko diskriminierender automatisierter Entscheidungen zu verringern,

13. Fahrzeuge mit datenschutzfreundlichen Fahrmodi als Standardeinstellung auszustatten,

14. Datenschutzfolgenabschätzungen für die Entwicklung und Umsetzung dieser neuen, innovativen und risikoreichen Technologien durchzuführen,

15. die Achtung der Privatheit personenbezogener Daten der Fahrzeugnutzer durch die für die Datenverarbeitung Verantwortlichen und die angemessene Berücksichtigung möglicher Verletzungen der Privatsphäre durch die Verarbeitung und Nutzung personenbezogener Daten zu fördern und

16. in einen Dialog mit den Beauftragten für den Datenschutz und für die Privatsphäre einzutreten zwecks Entwicklung von Compliance Tools, die Datenverarbeitungen im Zusammenhang mit vernetzten Fahrzeugen begleiten und diesbezüglich Rechtssicherheit bieten.