International Working Group
on Data Protection
in Telecommunications

675.42.20 4. April 2011

**Arbeitspapier**

# Datenaufzeichnung in Fahrzeugen (Event Data Recording - EDR):

# Fragestellungen zu Datenschutz und zum Schutz der Privatsphäre für Regierungen und Hersteller

*49. Sitzung, 4. - 5. April 2011, Montreal (Kanada)*

## Hintergrund

1. Der rasante technologische Fortschritt in der Informationsgesellschaft, insbesondere im Bereich Intelligente Verkehrssysteme (IVS), hat eine zunehmende Verarbeitung personenbezogener Daten in Fahrzeugen (PKW und LKW) sowohl für private als auch für kommerzielle Zwecke zur Folge.

2. Die nahezu allgegenwärtige Internetanbindung und immer größere Bandbreiten ermöglichen eine permanente Vernetzung sogenannter „Smart Vehicles“ (Intelligente Fahrzeuge) und somit den Zugriff auf angefallene Daten. Diese alarmierende technische Entwicklung führt zu einer Eingliederung intelligenter Fahrzeuge in das sog. „Internet of Things“, das die Verknüpfung von physischen Objekten, also Sachen, mit einer virtuellen Repräsentation in einer Internet-ähnlichen Struktur beschreibt.

3. Ohne geeignete Maßnahmen zum Schutz der Privatsphäre wird es weder Fahrern noch Passagieren solcher „Smart Vehicles“ möglich sein, die Verarbeitung ihrer Daten zu kontrollieren oder zu überwachen. Sie werden sich dieser Verarbeitung vielmehr gar nicht bewusst sein.

4. Ungeachtet der mannigfaltigen Erscheinungsformen technologischer Anwendungen in Fahrzeugen behandelt dieses Arbeitspapier ausschließlich die Aspekte der Datenaufzeichnung.

## Datenaufzeichnung in Fahrzeugen (EDR): Definitionen und Fakten

5. Im Moment eines Unfalls oder sonstigen Schadenseintritts werden verschiedene, durch Sensoren erfasste Daten mittels eines in das Fahrzeug eingebauten Geräts, dem „Event Data Recorder“ (EDR) oder auch Unfalldatenspeicher, gespeichert. Diese Geräte verarbeiten die Daten typischerweise innerhalb eines begrenzten Zeitraums im Zusammenhang mit einem Schaden, Unfall oder sonstigen Störfall verarbeitet (unmittelbar vor, während und nach dem Ereignis).

6. Der EDR kann sowohl ab Werk als auch nachträglich in das Fahrzeug eingebaut werden. Die gespeicherten Daten können mittels spezieller, für Endverbraucher meistens nicht frei

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

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

verkäuflicher Software heruntergeladen werden.

7. Die im Schadensfall gesammelten und registrierten Daten beziehen sich nicht ausschließlich auf technische Gegebenheiten des Fahrzeugs (wie etwa den Kraftstoffverbrauch oder die Funktionsfähigkeit des Airbags) und den Schadenszeitpunkt, sondern lassen darüber hinaus (direkt oder indirekt) Rückschlüsse auf das Fahrerverhalten zu (z.B. Bremsöldruck zu Beginn und Ende des Bremsvorgangs, Geschwindigkeit, Bremsverhalten, Motordrehzahl, Gaslast, Verwendung oder Nichtverwendung von Sicherheitsgurten).

8. Es handelt sich somit um personenbezogene Daten des Fahrers und ggf. auch der Passagiere (z.B. hinsichtlich der Daten über die Benutzung des Sicherheitsgurtes).

**EDR in Verbindung mit anderen „On-Board-Systemen“**

9. Im Rahmen vertraglicher Vereinbarungen mit Mobilfunkanbietern sind die EDRs mit den im Fahrzeug verbauten Kommunikationssystemen verbunden, die im Falle eines entsprechenden Vorfalls die relevanten Informationen an bestimmte Empfangsstationen übermitteln. Die Übermittlung erfolgt durch ein Unfallerkennungssystem (oder eingebautes Notrufsystem), das zu diesem Zweck automatisch oder auch manuell aktiviert wird. In den USA[1] und der EU[2] wurden bereits Initiativen ins Leben gerufen, die den Einbau dieser Systeme und die Einführung allgemeiner technischer Standards in den verschiedenen Transportsektoren befördern sollen.

10. Um mehr Beweismaterial zu einem Unfall zu erhalten, operieren EDRs vereinzelt auch mit eingebauten Videokameras (sog. Video Event Data Recorder – VEDR), wodurch nochmals erheblich mehr Informationen über das Verhalten des Fahrers sowie über an dem Unfall beteiligte Dritte gespeichert werden.

**Personenbezogene Fahrerdaten Daten beim Einsatz von EDR**

11. Personenbezogene Fahrerdaten, die mittels EDR bzw. VEDR insbesondere im Zusammenhang mit elektronischen Kommunikations- und Lokalisierungssystemen gesammelt wurden, lassen sich von einer stetig wachsenden Anzahl von Interessengruppen zu den verschiedensten Zwecken verwenden:
    a. Hersteller, Fahrer (ebenso wie andere, in Verkehrsunfälle verwickelte Personen), Eigentümer (z.B. Autovermieter oder Firmenflottenverwalter) und Versicherungsgesellschaften könnten die EDR-Daten nutzen, um bei Rechtsstreitigkeiten Zeugenaussagen zu überprüfen;
    b. Polizei und andere Behörden (z.B. könnte die für die Sicherheit des Straßenverkehrs zuständige Behörde die Informationen zur Vervollständigung der Beweislage bei einem Verkehrsunfall nutzen);
    c. Arbeitgeber, aus organisatorischen und Sicherheitsgründen;
    d. Versicherungsgesellschaften, zur Einteilung der Kunden in spezifische Tarifgruppen (z.B. nach der Fahrweise oder nach Regionen, in die gefahren wird);

---

1 Die US National Highway Traffic Safety Administration (NHTSA) hat im August 2006 entschieden, dass Hersteller nicht verpflichtet sind, EDRs in Neufahrzeuge einzubauen. Dennoch verlangt die NHTSA von den Herstellern den Einbau von EDRs, um jedenfalls einen Mindestdatensatz speichern zu können. Dieser soll 15 Typen von Unfalldaten beinhalten, darunter: Geschwindigkeit vor dem Unfall, Gaslast, Bremsverhalten, Geschwindigkeitsveränderungen, Sicherheitsgurtnutzung, Status der Airbag-Kontrolllampe und die Airbagauslösungszeit. Die Hersteller müssen sich mit diesen Standards bis September 2012 einverstanden erklären. http://www.nhtsa.gov/EDR

2 Zur „E-call Intiative“ der Europäischen Union im Einzelnen: Mitteilung der Europäischen Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, eCAll: Time for Deployment, Brüssel, 21.8.2009, KOM(2009) 434 endg.;
http://ec.europa.eu/information society/activities/esafety/ecall/index de.htm .

e. Forschung, zur Verbesserung der Verkehrsinfrastruktur;
f. Werbe- und Marketingagenturen könnten auf Grundlage der Daten Verhaltensanalysen durchführen, um so spezifisch zugeschnittene Angebote zu platzieren;
g. andere Dienstleister (z.B. Pannenhilfe).

12. Die oben aufgeführten Entwicklungen erfordern besonders sorgfältige Überlegungen in Bezug auf den Datenschutz und die Persönlichkeitsrechte sowohl der Fahrer als auch aller potentiellen Passagiere. Ein angemessener Ausgleich mit anderen individuellen Rechten und Interessen und mit dem öffentlichen Interesse an der Sicherheit des Straßenverkehrs muss erreicht werden.

13. Die Europäische Kommission hat 2008 eine Mitteilung betreffend einen Aktionsplan[3] zum Thema Intelligente Verkehrssysteme veröffentlicht. Gleichzeitig hat die Kommission eine entsprechende Richtlinie vorgeschlagen, die kürzlich durch den Rat und das Europäische Parlament verabschiedet wurde[4]. Diese Richtlinie, die bis Februar 2012 durch die Mitgliedsstaaten umgesetzt werden muss, verlangt beim Einsatz intelligenter Verkehrssysteme die Verwendung anonymer Daten, soweit dies angemessen ist[5]. Der Datenschutz und ein verantwortungsvoller Umgang mit den gesammelten Informationen sind in dem Aktionsplan wie in der Richtlinie von zentraler Bedeutung, um das Ziel effizienterer, umweltfreundlicher und sichererer Mobilität im Fracht- und Passagierverkehr innerhalb der Europäischen Union zu erreichen.

14. Durch das Rahmenprogramm für Forschung und technologische Entwicklung in der Europäischen Union wurde eine Vielzahl von Forschungsprojekten aufgelegt, die inzwischen teilweise abgeschlossen sind oder immer noch andauern, um die Sicherheit auf den Straßen zu erhöhen[6]. In einigen Jurisdiktionen wurden Gesetzesvorschläge entwickelt[7], in anderen sogar bereits Gesetze verabschiedet, die (unter anderem) auf den Schutz der Privatsphäre des Fahrers im Zusammenhang mit dem Einsatz von EDR abzielen[8] [9].

15. Zeitgleich wird von Seiten der Datenschutzbeauftragten ein Anstieg der EDR-Verwendung zur Verwaltung von Fahrzeugflotten registriert.[10] Im Rahmen der europäischen E-call Initiative hat die Artikel 29-Datenschutzgruppe bereits eine Reihe von Empfehlungen unterbreitet[11].

---

3 Aktionsplan zum Einsatz intelligenter Verkehrssysteme In Europa (COM(2008) 886).

4 Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern, Abl. L 207/1, 2010.

5 Art. 10 Abs. 3 der Richtlinie 2010/40/EU.

6 Vgl. Intelligent Car Brochure, p. 16 auf: http://ec.europa.eu/information_society/activities/intelligentcar/docs/right_column/intelligent_car_brochure.pdf .

7 Vgl. für die bundesstaatliche Ebene den Vorstoß durch *The Motor Vehicle Safety Act of 2010 (H.R. 5381).*

8 Kalifornien war der erste Staat, der gesetzlich verfügt hat, dass die Hersteller ihren Kunden gegenüber den Einbau von EDRs oder „black boxes" offenbaren müssen. Zur Gesetzgebung in Bezug auf Privatsphäre im Zusammenhang mit Datenaufzeichnung in Fahrzeugen siehe die Website der National Conference of State Legilatures auf: http://www.ncsl.org . Detaillierte Informationen zum aktuellen Stand in Sachen Datenaufzeichnung in Fahrzeugen in den U.S.A. finden sich auf der Seite der National Highway Traffic Safety Administration (http://www.nhtsa.gov/EDR ).

9 Vgl. für die bundesstaatliche Ebene den Vorstoß durch *The Motor Vehicle Safety Act of 2010 (H.R. 5381).*

10 Französische Datenschutzbehörde (CNIL), Délibération n° 2006-066 du 16 mars 2006 portant adoption d'une recommendation relative à la mise en oeuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme public ou privé; Délibération 2010-096 du 8 avril 2010 portant recommandation relative à la mise en oeuvre, par les compagnies d'assurance et les constructeurs automobiles, de dispositifs de géolocalisation embarqués dans les véhicules; Italienische Datenschutzbehörde (Garante per la protezione dei dati personali) on Geolocation in Public Transportation and Passenger Security, 5 June 2008, http://www.garanteprivacy.it , doc. no. 1672796

11 Artikel 29-Datenschutzgruppe, Working document on data protection and privacy implications in eCAll initiative, WP 125, http//ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp125_de.pdf

16. Die anstehende umfassende Einführung dieser Systeme, die Komplexität der Materie sowie die absehbaren notwendigen Investitionen (möglicherweise auch in Hinsicht auf die Verkehrsinfrastruktur) bedingen die dringliche Notwendigkeit eines klaren Regelwerkes, dem gleichwohl eine ausführliche öffentliche Auseinandersetzung mit der Thematik vorausgehen sollte. Der Entwicklung und Ausgestaltung eines solchen Regelwerkes sollte der Gedanke innewohnen, den Datenschutz von vornherein in die Gesamtkonzeption einbeziehen, anstatt Datenschutzprobleme im Nachhinein mühsam und mit viel Zeitaufwand durch Korrekturprogramme beheben zu wollen[12].

17. Vor diesem Hintergrund

**ruft die Arbeitsgruppe die Regierungen dazu auf,**

a) in Zusammenarbeit mit den Datenschutzbeauftragten und den betreffenden Interessenvertretern aus Industrie und Wirtschaft, ein angemessenes gesetzgeberisches Regelwerk darzulegen, zu definieren bzw. zu bestätigen (damit die Verarbeitung personenbezogener Daten auf gesetzmäßige Weise erfolgt und Missbrauch der durch EDR und möglicherweise andere intelligente Technologien in Fahrzeugen gesammelten und/oder übermittelten Daten ausgeschlossen oder eingeschränkt wird,

b) die Umsetzung der erforderlichen technischen Standards zu fördern und zu unterstützen, und

**empfiehlt:**

*I. Transparenz*

Jedwede Verwendung von Daten, die durch EDRs (oder andere intelligente Technologien) entstanden sind, sollte für den Fahrzeugeigentümer sowie die jeweiligen Fahrzeugnutzer in vollem Umfang transparent sein. Die Nutzer sind in die Lage zu versetzen, sich auf einfachstem Wege ein vollständiges Bild über die Erhebung und Speicherung sowie den Zweck der Verwendung aller sie betreffenden persönlichen Informationen machen zu können.

Zu diesem Zweck sollten:

a. *Hersteller/Systemintegratoren* ihre Kunden sorgfältig über die Verarbeitung personenbezogener Daten einschließlich der Möglichkeiten der Fahrzeugpositionsbestimmung aufklären. In dem Fahrzeug sollte ein (schriftlicher oder stimmlicher) Hinweis erfolgen. Ausdrückliche und detaillierte Informationen sollten im Benutzerhandbuch vorhanden sein.
b. *Datenverarbeitende Stellen* (wie etwa Arbeitgeber, Versicherer, Autovermietungen etc.) die Nutzer vollständig über (i) den Zweck der Verarbeitung erhobener Daten; (ii) die Kategorie(n) zu verarbeitender personenbezogener Daten; (iii) die Empfänger bzw. die Kategorien der Empfänger der Daten; und (iv) ihre Zugriffsrechte informieren.

*II. Einwilligung des Eigentümers*

Jegliches zur Speicherung personenbezogener Daten fähiges Gerät sollte regelmäßig nur nach der freiwilligen Einwilligung des ausführlich informierten Eigentümers und nach ausdrücklichem Hinweis an den Nutzer aktiviert werden. Zwingend notwendige Einbauten, die geeignet sind, personenbezogene Daten zu speichern oder an Dritte zu übermitteln, bedürfen einer gesetzlichen Grundlage, aus der vorgesehene Zweck der Speicherung personenbezogener Daten eindeutig hervorgeht.

*III. Datenqualität*

12 Vgl. ISO/TR Technical Report 12859 on Intelligent transport systems - System architecture - Privacy aspects in ITS standards and systems.

Die Datenaufzeichnung sollte nur solche personenbezogene Daten umfassen, deren Verarbeitung im Verhältnis zu dem Zweck ihrer Verarbeitung erforderlich und angemessen ist. Der Nutzung anonymisierter Daten sollte der Vorzug gegeben werden, wo immer dies möglich ist.

Entscheidungen anlässlich besonderer Vorkommnisse in Zusammenhang mit dem Fahrzeug sollten nicht ausschließlich von den Informationen aus der Datenaufzeichnung abhängig gemacht werden. Zu Zwecken der Qualitätsanalyse sind die aufgezeichneten Daten durch ausgewiesene Sachverständige zu prüfen und sorgfältig unter Heranziehung weiterer Nachweise und Begleitumstände abzugleichen.

*IV. Privacy by Design*

Das Leitmotiv bei der Entwicklung und Einführung von Systemen zur Datenaufzeichnung in bzw. der Interaktion mit Fahrzeugen sollte es sein, den Datenschutz und den Schutz der Privatsphäre von vornherein in die Gesamtkonzeption einzubeziehen. Derartige Systeme sollten darauf ausgerichtet sein, die Notwendigkeit der Verarbeitung personenbezogener Daten zu minimieren und zugleich einen potentiellen Missbrauch personenbezogener Daten zu verhindern.

*V. Zugriff auf (personenbezogene) Daten*

Vor einer Einführung ist das Augenmerk auf den Schutz der Privatsphäre zu richten und klar festzulegen, wer unter welchen Voraussetzungen (z.B. Richtervorbehalt) auf die aufgezeichneten personenbezogenen Daten zugreifen darf. Dies gilt insbesondere in Hinsicht auf solche personenbezogenen Daten, die nicht ausschließlich vom Fahrer stammen. Ihm selbst ist das freie und vollumfängliche Zugriffsrecht auf seine eigenen Daten grundsätzlich zuzuerkennen. Hinsichtlich aller anderen Personen, deren personenbezogene Daten aufgezeichnet werden könnten, sollten klare und zweckmäßige Methoden zur Wahrung und ggf. Durchsetzung ihrer Rechte bereitgestellt werden. Eine vorherige Folgenabschätzung in Bezug auf den Datenschutz und den Schutz der Privatsphäre ist ein nützliches Instrument für eine solche Analyse.

*VI. Datensicherheit und -integrität*

Standardisierte Sicherheitsmaßnahmen zur Vermeidung unrechtmäßigen Zugriffs, Verlustes oder rechtswidriger Veränderung der aufgezeichneten Daten müssen festgelegt und universell umgesetzt werden. Um das Risiko unerwünschter Datentransfers und anderer schwerwiegender Angriffe von außen zu verringern, sollten zusätzlich verlässliche Verschlüsselungstechniken und Authentifizierungssysteme verwendet werden. Für den Endverbraucher sollte klar erkennbar sein, dass die im Fahrzeug verbauten Systeme zur Datenaufzeichnung und -übermittlung diesen Standards vollauf gerecht werden. Im Zusammenhang untereinander vernetzter Systeme sind entsprechende Sicherheitsmaßnahmen sogar von noch größerer Bedeutung.

*VII. Überwachung von Arbeitnehmern*

Darüber hinaus sind gesetzliche Regelungen zum Schutz von Arbeitnehmern vor Überwachung durch den Arbeitgeber zu beachten und zu respektieren, wenn dieser Systeme installiert, die der Verhaltenskontrolle von Arbeitnehmern oder der Ortung der Fahrzeugposition dienen (z.B. Fahrtenschreiber oder Lokalisierungsdienste).