Datenschutz in IVS

Anna Sinitsyna

Zentrum für Angewandte Rechtswissenschaft (ZAR)
Betreuender Mitarbeiter: Ref. iur. Leonie Sterz

Abstract

Abbildungsverzeichnis

1 Einleitung

Motivation

In näher Zukunft werden nach und nach im Alltag Fahrzeuge eingeführt, die miteinander (Car-to-Car, kurz C2C) und mit der Infrastruktur (Car-to-Infrastructure, kurz C2I) kommunizieren können. Der Oberbegriff zu dieser Art der Kommunikation lautet Car-to-X (C2X). Der Datenaustausch in solchen Kooperativen Intelligenten Systemen (C-ITS) findet statt, um Unfälle auf den Straßen zu vermeiden und damit die Sicherheit im Straßenverkehr zu gewährleisten. Dafür senden Fahrzeuge gegenseitig verkehrsrelevante Daten, wie zum Beispiel Beschleunigung, Geschwindigkeit, Länge und Gewicht des Fahrzeugs. Diese Daten werden verwendet, um ein Verkehrslagebild zu erstellen und zu verteilen, damit teilnehmende Fahrzeuge stets die aktuellsten Informationen besitzen und auf eintretende Verkehrssituationen geeignet reagieren können.

...[12]

Neue Problemstellung, wozu braucht man Datenschutz und Privacy? Was ist das Ziel der Seminararbeit?

Integrität und Vertraulichkeit!

2 Hintergrund

IVS-RL unbedingt einführen!!!

Begriff C-ITS - [9], andere Begriffe einführen.

Initiativen in Deutschland und EU, Geschichte und Entwicklung

Car-2-Car Communication Consortium - [2]

Related work - Literatur, die sich mit der Fragenstellung beschäftigt - z.B. [6]

Die EU hat bereits vor zehn Jahren eine Rechtsgrundlage für intelligente Verkehrssysteme geschaf- fen. Es handelt sich um die RL 2010/40/EU v. 7.7.2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern (IVS- 2 RL).

Die Bundesrepublik Deutschland hat hinsichtlich der Umsetzung der IVS-RL und der Ausfüllung der delegierten Verordnungen die föderale Struktur zu beachten. Die Umsetzung der Richtlinie erfolgte 17 18 2013 durch das Gesetz über Intelligente Verkehrssysteme im Straßenverkehr , welches 2017 geändert wurde, um den Anforderungen der delegierten Verordnungen zu genügen. - Jochum: Verkehrsdaten für intelligente Verkehrssysteme ZD 2020, 497

3 Technische Funktionsweise der C2C-Kommunikation

Im folgenden Abschnitt wird die Funktionsweise der C2C-Kommunikation und die dafür benötigte Infrastruktur näher beschrieben. Der Nachrichtenaustausch zwischen Fahrzeugen beruht auf Public-Key Kryptografie, somit werden die Nachrichten mit einer Signatur und einem Zertifikat versehen, die von einer zentralen Stelle ausgegeben werden. Eine kryptographische Signatur ist (analog zu einer Unterschrift) eine Bestätigung, dass die Nachricht tatsächlich von dem Versender stammt und nicht auf dem Weg verändert wurde. Der Empfänger kann dies überprüfen, in dem er die zentrale Stelle kontaktiert und eine Authentizität-Anfrage macht. Die Integrität der Nachricht kann er direkt durch die Signatur verifizieren. Allerdings werden die Nachrichten selbst nicht verschlüsselt und können von allen Verkehrsteilnehmern gelesen werden. Das heißt, dass alle darin enthaltenen Daten ebenfalls von jedem mitgelesen können, was zu datenschutzrechtlichen Problemen führen könnte.

Im Abschnitt 3.2 wird auf die Nachrichtenformate der C2C-Kommunikation eingegangen, sowie auf die darin gespeicherten Daten, die möglicherweise zur Identifikation des Fahrzeugs benutzt werden können. Dieses technische Thema bildet eine Grundlage für Herstellbarkeit des Personenbezugs aus den Fahrdaten, deren Möglichkeit in weiteren Kapiteln analysiert wird.

Des Weiteren werden mögliche Angriffe auf die Pseudonymität der Nachrichten aufgeführt, aufgrund deren Bewegungsprofile von Fahrzeugen erstellt werden können. Aktuell

ist die Infrastruktur so konstruiert, dass Fahrzeuge Nachrichten und Zertifikate pseudonym versenden, und keine Zuordnung von mehreren über einen längeren Zeitraum versendeten Nachrichten zu einem Fahrzeug technisch möglich ist. Allerdings gibt es andere Methoden, wodurch solch eine Zuordnung ohne Zustimmung des Fahrers realisiert werden kann, diese werden im Abschnitt 3.3 beschrieben.

3.1 Public-Key Infrastruktur

Um den oben genannten Nachrichtenaustausch zu ermöglichen, braucht man eine entsprechende Public-Key Infrastruktur (PKI), die aus einer oder mehreren Certification Authorities (CAs) besteht. Eine CA ist eine zentrale Stelle die in der Lage ist, digitale Zertifikate zu produzieren, diese Zertifikate den End-Entitäten zu erteilen und später ihre Authentizität zu verifizieren. Als End-Entitäten versteht man ITS-Stationen (u.a. Fahrzeuge), die die erstellten Zertifikate für die Kommunikation untereinander verwenden. Es gibt zwei Arten von Zertifikaten: ein langlebiges Enrolment Credential (EC) und ein kurzzeitgültiges Authorization Ticket (AT). Die Pseudonymität des Datenaustauschs wird durch ständigen Wechsel des ATs gewährleistet, womit die Nachricht signiert wird. Der EC wird hingegen nicht mit der Nachricht übertragen und ist nur den PKI Komponenten bekannt [12].

Die PKI wird aus drei Stufen zusammengesetzt [10]:

- Root-CAs (erstellen Zertifikate für untergeordnete CAs)
- Mindestens zwei Sub-CAs
- End-Entitäten (EEs)

Darüber hinaus gibt es zwei Arten von Sub-CAs: Enrolment Authorities (EA) und Authorization Authorities (AA). Die EAs erstellen langlebige Zertifikate für EEs, die für die Authentifizierung innerhalb der PKI verwendet werden (ECs). Die AAs hingegen stellen kurzzeitige Zertifikate zur Verfügung, mit denen die EEs (z.B. Fahrzeuge) untereinander kommunizieren können ohne die Pseudonymität von einzelnen Entitäten zu verletzen (ATs). Der schematische Aufbau von einer PKI wird in der Abbildung 1 verdeutlicht.

Bevor jegliche Kommunikation stattgefunden hat, muss sich die End-Entität zunächst bei der zugehörigen EA registrieren und ein Enrolment Credential (EC) erhalten, das mehrere Jahre gültig ist. Die EA bekommt dabei die Registrierungsinformationen von der EE, zum Beispiel ihre Fahrzeugidentifizierungsnummer und ihren öffentlichen Schlüssel. Diese Information wird verschlüsselt übermittelt und ist nicht öffentlich verfügbar. Die EE signiert den initialen Zertifikatsrequest mit ihrem eingebauten privaten Schlüssel und übermittelt ihn an die EA. Falls die Daten übereinstimmen, erhält die EE einen Enrolment Credential.

Mit einem validen EC kann die EE weiterhin kurzzeitgültige Authorization Tickets (AT) bei der AA beantragen. ATs sind wie vorhin beschrieben kurzzeitgültige Zertifikate für C2X Kommunikation, die oft gewechselt werden und somit der Senderpseudonymität

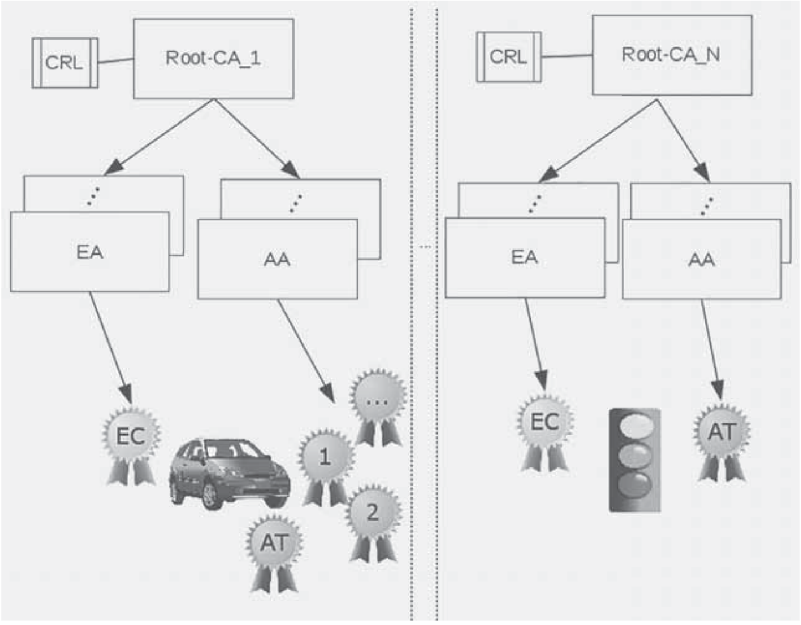

Abbildung 1: Aufbau einer PKI für C2X Kommunikation nach [12]

dienen. Die Nachrichten sollten keinen eindeutigen Identifikator erhalten, damit kein Personenbezug hergestellt werden kann. Daher werden sie mit ATs signiert und nicht mit den langlebigen ETs, die für ein Fahrzeug über mehrere Jahre gültig ist.

Ein AT wird von einer Entität bei der AA beantragt. Die Anfrage an die AA enthält unter anderem verschlüsselte Daten, die nur von der entsprechenden EA ausgelesen werden können [5], darunter das langlebige EC von der Entität. Eine AA kann diese Daten nicht auslesen, da sie verschlüsselt sind, also leitet sie diesen Teil der Anfrage an die zugehörige EA. Die EA entschlüsselt die Daten, bestätigt die Authentizität der EE mit dem angehängten EC und schickt eine Statusmeldung an die AA, ohne diese zusätzliche Information preiszugeben. Es ist wichtig, die EA und AA organisatorisch getrennt zu halten, da sonst bei der AT-Anfrage eine Zuordnung zu der End-Entität bzw. ihrem EC möglich wäre.

Nachdem die mit dem AT signierte Nachricht erfolgreich an die empfangende EE übermittelt wurde, nutzt sie den AT um die Nachricht zu verifizieren. Dies erfolgt mittels einer Kettenprüfung durch die AA und die entsprechende Root-CA, wodurch die Authentizität der Nachricht festgestellt wird.

In Europa ist zusätzlich zu der oben beschriebenen PKI eine globale Vertrauensliste vorgesehen, die innerhalb der europäischen Grenzen alle vertrauenswürdige Root-CA-Zertifikate beinhaltet. Diese wird von einem zentralen Trust List Manager (TLM) erstellt und elektronisch signiert. Somit wird die Interoperabilität von europäischen PKIs über Grenzen sichergestellt, was durch die IVS-RL vorgeschrieben wird[1]. Darüber hinaus ist es wichtig, die nicht mehr vertrauenswürdigen Zertifikate zurückziehen zu können - dies

[1] *Jochum*, ZD 2020, 497

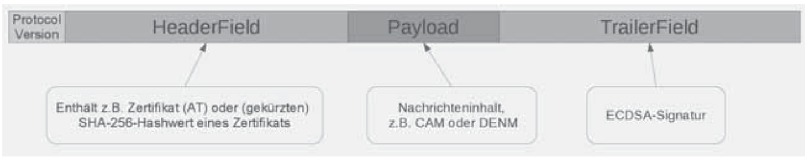

Abbildung 2: Grobaufbau einer verschlüsselten Nachricht nach [12]

wird durch sogenannte Certificate Revocation Lists (CRL) sichergestellt. Diese werden allen PKI-Teilnehmern von der jeweiligen Root-CA zur Verfügung gestellt und enthalten die Liste mit allen revozierten Zertifikaten.

3.2 Nachrichtenformate

Die Nachrichtenformate, die für die oben beschriebene PKI nötig sind, wurden von dem Europäischen Institut für Telekommunikationsnormen (ETSI) definiert. Im Weiteren wird auf [5] verwiesen, in dem die Paketstruktur für gesicherte C2X-Nachrichten und deren Zertifikatsformat festgelegt wurde.

Der grobe Aufbau einer gesicherten C2X-Nachricht wird in der Abbildung 2 dargestellt. Sie enthält unter anderem die ECDSA-Signatur ([1]), den Verifikationsschlüssel des Senders und die eigentliche Nachricht, die im Payload gespeichert ist. Für die Car-2-Car Kommunikation sind zurzeit zwei Nachrichtenformate vorgesehen:

- die Cooperative Awareness Message (CAM) und die
- Decentralized Environmental Notification Message (DENM) [13].

Im Weiteren wird nur die CAM betrachtet, da die DENM keine personenbezogenen Daten beinhaltet und im datenschutzrechtlichem Sinne kein Problem darstellt [7]. Der Aufbau einer CAM wird in der Abbildung 3 dargestellt. Sie besteht aus vier Elementen: Header, CAM Information, Signature und Certificate. Die tatsächliche Information über das Fahrzeug wird im Block CAM Information gespeichert. Er beinhaltet sowohl dynamische Daten (z.B. Last Geographic Position, Speed) als auch statische Daten über das Fahrzeug, die trotz ständigem Pseudonymwechsel identisch bleiben (z.B. Length, Weights). Eine CAM erhält keinen primären Identifikator, aufgrund dessen eine eindeutige Zuordnung zum Fahrzeug möglich wäre.

3.3 Angriffsmöglichkeiten

Auch wenn CAMs keine primären Identifikationsmerkmale erhalten, existieren es mehrere Möglichkeiten, um mehere CAMs von einem Fahrzeug miteinander zu verbinden und damit ein Bewegungsprofil von diesem Fahrzeug zu erstellen. Dies kann zu diversen Risiken für die Privatsphäre führen, falls der Personenbezug von diesen Fahrdaten hergestellt werden kann, da der gesamte Fahrweg einer Person offengelegt wird. Im folgenden Ab-

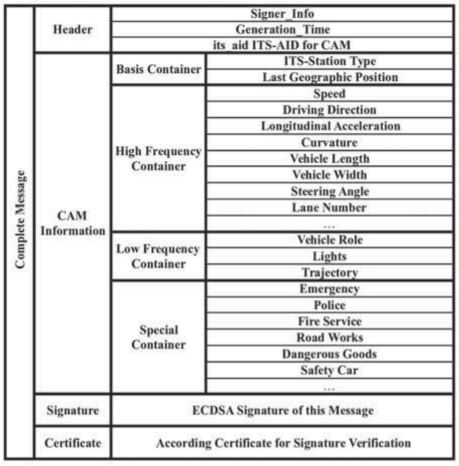

Abbildung 3: Detallierter Aufbau einer CAM nach [7]

schnitt werden einige Angriffsarten auf die Pseudonymität von CAMs näher beschrieben und analysiert.

Als erstes Beispiel sei ein sogenannter 'Big Brother Angreifer' angeführt, der eine Infrastruktur von Empfangseinrichtungen in einer geografischen Region betreibt und in der Lage ist, in dieser Gegend CAMs von Fahrzeugen zu erfassen und auszuwerten. Das wäre möglich, indem der Angreifer zum Beispiel eine Fahrzeug-Flotte aufstellt, die eingehende CAMs an einen zentralen Server übermittelt. Auch wenn vorbeifahrende Fahrzeuge ihr Pseudonym jede zehn Sekunden ändern würden, könnten sie mit solch einer Infrastruktur verfolgt werden [16]. Da diese Art von Überwachung alle Fahrzeugdaten in der Gegend erfassen würde, könnte sie für breitere Verkehrsanalysen genutzt werden.

Darüber hinaus gibt es einige Möglichkeiten, die Bewegungen von einzelnen Fahrzeugen detailliert aufzuzeichnen. Zum Beispiel kann man mithilfe eines sich mit dem Fahrzeug bewegendes Überwachungstools sogenannte CAM-Traces erstellen, d.h. die gefahrene Strecke eines Fahrzeugs und alle von ihm auf dieser Strecke erstellten CAMs. Auch wenn das Fahrzeug regelmäßig seinen Signaturschlüssel wechselt, würde es reichen, nur eine CAM aus der CAM-Trace dem Fahrzeug eindeutig zuzuordnen, um die gesamte CAM-Trace diesem Fahrzeug zuzuordnen [7].

Es existiert eine Reihe von Methoden, um diese Zuordnung technisch durchzuführen. In [14] wurde dargelegt, dass sie aufgrund der sog. Secondary Vehicle Identifier erfolgen kann. Diese wird von diversen drahtlosen Schnittstellen im Auto zur Verfügung gestellt (z.B. eine Headunit, die eine öffentliche Bluetooth-Schnittstelle mit einem nutzerfreundlichen Namen besitzt). Die Secondary Vehicle Identifiers sind einfach zu erfassen und können einer eindeutigen Zuordnung der empfangenen CAM-Trace zum Fahrzeug dienen.

...andere Möglichkeiten?

4 Vereinbarkeit mit datenschutzrechtlichen Prinzipien

Die Datenschutzgrundverordnung (DSGVO) ist eine Verordnung, mit der die Regeln zur Verarbeitung personenbezogener Daten in der Europäischen Union vereinheitlicht werden. Sie ist am 25. Mai 2018 inkraft getreten und hat zu dem Zeitpunkt geltende Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ersetzt.

In diesem Abschnitt wird diskutiert, ob die Erhebung von Fahrdaten in einer PKI ein datenschutzrechtliches Problem darstellt, und geprüft, ob die DSGVO in diesem Fall anwendbar ist. Dafür werden einige Verfahren vorgestellt, mithilfe von denen ein Bewegungsprofil und deren Personenbezug aus den Fahrdaten hergestellt werden kann. Darüber hinaus

Warum stellen IVS ein datenschutzrechtliches Problem dar? Ist DSGVO anwendbar?

(Beispiel von rechtlicher Probl emstellung und Richtlinien zu deren Lösung - [3]) - wird wahrscheinlich nicht behandelt oder kurz erwähnt, da wir uns auf DSGVO konzentrieren

4.1 Anwendbarkeit der DSGVO

Zunächst wird die Anwendbarkeit der DSGVO auf die in CAMs erhaltene Fahrdaten diskutiert. Falls diese Daten personenbezogen sind, beziehungsweise für eine eindeutige Identifizierung der Person benutzt werden können, fällt ihre Verarbeitung unter DSGVO und somit sind sämtliche Grundsätze anwendbar, wie zum Beispiel Grundsatz der Datenminimierung und Grundsatz der Integrität und Vertraulichkeit.

4.1.1 Bewegungsprofile und Verhaltensprofile

Wie in Kapitel 3.3 erwähnt, erhalten CAMs keine primären Identifikationsmerkmale, jedoch ist es möglich, mithilfe von einer geeigneten Infrastruktur Bewegungsprofile von Fahrzeugen zu erstellen. Außerdem enthalten CAMs statische Attribute wie zum Beispiel die Fahrzeuglänge und dessen Gewicht, die eine zusätzliche Kennzeichung von einem Fahrzeug erlauben. So wäre es unter Umständen möglich, ein bestimmtes Modell von einem bestimmten Hersteller nur aus der CAM zu erkennen. In wenig befahrenen Gebieten kann dies zu einer eindeutigen Identifizierung von dem Fahrzeug und einer Zuordnung zum ganzen CAM-Trace führen. Darüber hinaus kann man mithilfe von Secondary Vehicle Identifiers (z.B. einer öffentlich verfügbaren Bluetooth-Schnittstelle) diese Zuordnung durchführen. Letztens, da die CAM-Daten mit einer hohen Frequenz versendet werden, kann der Fahrweg mit einer hohen Zuverlässigkeit vorausberechnet und zurückberechnet werden.

Somit ist es grundsätzlich möglich, aus einem flächendeckenden Datenbestand aus CAMs über einen längeren Zeitraum Bewegungsprofile zu erstellen, und somit gegebenenfalls auch Verhaltensprofile. In [4] wurde zum Beispiel nachgewiesen, dass anhand der Lenkbewegungen ruhige von nervösen Fahrer unterschieden werden können. Außerdem wäre es durch die Anwendung von künstlicher Intelligenz und maschinellem

Lernen durchaus möglich, große Datenbestände von Bewegungsprofilen und somit die zugehörigen Fahrer zu klassifizieren, falls Personenbezug hergestellt werden kann.

4.1.2 Herstellbarkeit Personenbezug

Nach Art. 4 Nr. 1 DSGVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Selbst wenn CAMs direkt keine primären Identifikationsmerkmale enthalten (z.B. die Fahrzeugidentifizierungsnummer), kann deren Personenbezug grundsätzlich mit Zusatzwissen hergestellt werden. Technisch kann das durch eine Auflösung des Pseudonyms bei einem sogenannten Pseudonym Provider erfolgen [7], aber auch durch andere Wege. Zum Beispiel, kann man anhand einer CAM-Trace aufgrund der am meisten gefahrenen Strecken den Wohn- und Arbeitsort einer Person identifizieren. Außerdem wäre es zum Beispiel möglich, durch Datenanalyse die Outliers in der Menge von den aufgezeichneten CAM-Traces identifizieren und versuchen, sie auf Personen mit entsprechendem Tagesablauf zurückzuführen. Besonders in wenig befahrenen Gebieten wäre diese Technik erfolgreich. Letztendlich wäre in vielen Situationen der einfachste Weg, vor Ort das Fahrzeug zu identifizieren (z.B. durch aufgezeichnete Videos oder Zeugenaussagen), und später aus dem Datenbestand die entsprechende CAM-Trace auszusuchen. Alle oben ausgeführten Techniken voraussetzen natürlich eine umfassende Erfassung von Fahrdaten und einen vorhandenen Bestand von Bewegungsprofilen (z.B. den in Kapitel 3.3 beschriebenen Big Brother Angreifer).

Eine besondere Sensibilität allein aus der Art der Daten wird nach Art. 9 EU-DSGVO nicht begründet [15].

Für die datenschutzrechtliche Betrachtung genügt bereits die abstrakte rechtliche Möglichkeit der Informationsverknüpfung, weshalb die Identifizierbarkeit des Fahrzeughalters unabhängig davon zu bejahen ist, ob die – ohnehin niederschwelligen – Voraussetzungen des Auskunftsanspruchs im konkreten Einzelfall tatsächlich erfüllt sind. ..... Sind im Kfz erhobene Daten mit dem Kennzeichen oder der Fahrzeug-Identifizierungsnummer verknüpft, ist jedenfalls im Hinblick auf den Fahrzeughalter von personenbezogenen Daten auszugehen ..... Diese Zuordnung mag freilich künftig zu überdenken sein, wenn sich Shared Mobility-Konzepte durchsetzen sollten, aufgrund derer die Nutzer von der Anschaffung eigener Fahrzeuge absehen und ihren Mobilitätsbedarf durch kurzzeitige Anmietung von Fahrzeugen gewerblicher Flottenbetreiber decken. [2]

[15] - Datenschutzrechtliche Analyse der Car-2-Car-Communication, guter Ausgangspunkt.

4.2 Grundsatz der Datenminimierung

Art.5 Abs.1c DSGVO - "Datenminimierung".

Geeignete Pseudonymisierung

[2] *Specht/Mantz*, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Aufl., 2019, Rn. 12, 13

4.3 Recht auf Datenübertragbarkeit

Art.20 DSGVO - "Recht auf Datenübertragbarkeit"

[8] - Analyse der Datenübertragbarkeit, Begründung der DSGVO-Anwendbarkeit

Art. 20 Abs. 1 DS-GVO gilt nur, wenn die personenbezogenen Daten vom Betroffenen bereitgestellt wurden

Separate section: wo werden Daten gesammelt? Wer sammelt Daten? -> MDM (Jochum)

Wer ist an den Daten interessiert? - Klink-Straub/Straub: Vernetzte Fahrzeuge – portable Daten (ZD 2018, 459) 460

4.4 Datenschutzmaßnahmen

Offene Fragen: welche Daten wo gesammelt wo gespeichert, wie erfassen? Wie Missbrauch vermeiden?

Dies entspricht den Vorgaben des Art. 10 IVS-RL. Die Richtlinie fordert, dass die Mitgliedstaaten sicherstellen, dass personenbezogene Daten gegen Missbrauch, d.h. insbesondere unrechtmäßigen Zugriff, Veränderung oder Verlust, geschützt und weitestgehend anonymisierte Daten für den Be- trieb von IVS-Anwendungen und -Diensten vorgesehen werden. In der Praxis bedeutet das, dass die Vorgaben der DS-GVO einzuhalten sind.

Damit enthalten die delegierten Verordnungen grundsätzliche Verpflichtungen zur Zurverfügungstel- lung bestimmter Daten ab einem bestimmten Zeitpunkt in bestimmten Formaten. Nicht geregelt ist allerdings, wer diese Daten einsammelt. Außerdem ergibt sich daraus nicht, ob die entsprechenden Adressaten diese Daten auch systematisch und vollständig sammeln und digitalisieren müssen. Bereitstellung von Daten auf Anforderung bedeutet jedenfalls nicht, diese Daten aktiv zu erheben und zu digitalisieren. Die delegierten Verordnungen verweisen i.Ü. nur auf den nationalen Sammelpunkt. Zwar macht das Unionsrecht formelle und materielle Vorgaben auch für die Weiterverwendung der Daten, wonach die Mitgliedstaaten vor allem sicherzustellen haben, dass bei der Verarbeitung per- sonenbezogener Daten die Grundrechte, die Grundfreiheiten und die Privatsphäre zu achten sind und jeglicher Missbrauch vermieden werden muss, vgl. Art. 10 IVS-RL. Außerdem fallen die Daten auch in den Anwendungsbereich der RL 2019/1024 v. 20.7.2019 über offene Daten und die Weiterver- Jochum: Verkehrsdaten für intelligente Verkehrssysteme (ZD 2020, 497) 500 wendung von Informationen des öffentlichen Sektors (vgl. Art. 1 Abs. 4 RL 2019/1024), weswegen die digitale Datenverarbeitung unter einem besonderen persönlichkeitsrechtlichen Schutz steht und damit im datenschutzrechtlich relevanten Bereich liegt. - Jochum: Verkehrsdaten für intelligente Verkehrssysteme ZD 2020, 499

Das schutzwürdige Interesse an der Vermeidung von Bewegungsprofilen besteht in jedem Fall; eine individualisierte Zweitnutzung setzt deshalb eine explizite Einwilligung voraus. (zweitnutzung - begehrlichkeit!)- [15]

[11] - alle o.g. Datenschutzmaßnahmen + öbligation to report a data breach, to conduct a data protection impact assessment". änalytical progress of AI". Guter Ausgangspunkt für Kapitel 4.1

Die in [7] aufgeführten Empfehlungen untersuchen und analysieren.

unentgeltlich

5 Zusammenfassung und Ausblick

...

Literatur

[1] Elaine Barker u. a. „NIST Special Publication 800-56A Revision 2 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography“. In: (2013). DOI: 10.6028/NIST.SP.800-56Ar3. URL: https://doi.org/10.6028/NIST.SP.800-56Ar3.

[2] *CAR 2 CAR Communication Consortium*. URL: https://www.car-2-car.org.

[3] *COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Commission Delegated Regulation supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems*. 2019. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019SC0096#_Ref521658883.

[4] Frank Dettki. *Methoden zur objektiven Bewertung des Geradeauslaufs von Personenkraftwagen*. 2005. URL: https://elib.uni-stuttgart.de/handle/11682/4059 (besucht am 24. 11. 2020).

[5] ETSI (European Telecommunications Standards Institute). *TS 102 941 - V1.2.1 - ITS; Security; Trust and Privacy Management*. Techn. Ber. 2018, S. 1–30.

[6] Jochum. „Car-to-Car-Communication zwischen Datenbegehrlichkeit und digitaler Selbstbestimmung“. In: *ZD 2020, 497* (2020).

[7] Michael Kiometzis und Markus Ullmann. „Fahrdaten für alle?“ German. In: *Datenschutz und Datensicherheit - DuD* 41.4 (März 2017), S. 227–232. DOI: 10.1007/s11623-017-0763-6.

[8] Klink-Straub/Straub. „Vernetzte Fahrzeuge – portable Daten“. In: *ZD 2018, 459* (2018).

[9] *MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN Eine europäische Strategie für Kooperative Intelligente Verkehrssysteme - ein Meilenstein auf dem Weg zu einer kooperativen, vernetzten und automatisierten Mobilität*. Techn. Ber. 2016.

[10] *Result of C-ITS Platform Phase II Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) RELEASE 1*. Techn. Ber. 2017. URL: https://ec.europa.eu/transport/sites/transport/files/c-its%7B%5C_%7Dsecurity%7B%5C_%7Dpolicy%7B%5C_%7Drelease%7B%5C_%7D1.pdf.

[11] Olga Seewald. „Regulation of data privacy and cybersecurity in connected and automated vehicles in the U . S . and the EU – Part 1 **“. In: (2018), S. 124–132.

[12] Thomas Strubbe, Nicolas Thenée und Christian Wieschebrink. „IT-Sicherheit in Kooperativen Intelligenten Verkehrssystemen“. German. In: *Datenschutz und Datensicherheit - DuD* 41.4 (März 2017), S. 223–226. DOI: 10.1007/s11623-017-0762-7.

[13] *TS 103 097 - V1.1.1 - Intelligent Transport Systems (ITS); Security; Security header and certificate formats*. Techn. Ber. 2013, S. 1–33.

[14] Markus Ullmann, Thomas Strubbe und Christian Wieschebrink. *Technical Limitations and Privacy Shortcomings of the Vehicle-to-Vehicle Communication*. c. 2016, S. 22–27. ISBN: 9781612085159.

[15] Thilo Weichert. „Car-to-Car-Communication zwischen Datenbegehrlichkeit und digitaler Selbstbestimmung“. In: *Svr* (2016), S. 361.

[16] B. Wiedersheim u. a. „Privacy in inter-vehicular networks: Why simple pseudonym change is not enough“. In: *2010 Seventh International Conference on Wireless On-demand Network Systems and Services (WONS)*. 2010, S. 176–183. DOI: 10.1109/WONS.2010.5437115.