universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

„Smart Cars und der Datenschutz“
Datenschleuder oder sinnvolle Datenverwendung?

verfasst von / submitted by

Mag. Franz Stingl

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2016 / Vienna, 2016

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	A 992 942
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Universitätslehrgang Informations- und Medienrecht
Betreut von / Supervisor:	a.o. Univ. Prof. Dr. Dietmar Jahnel

Inhaltsverzeichnis

Aus Gründen der sprachlichen Vereinfachung sind alle Aussagen in diesem Dokument als geschlechtsneutral zu verstehen.

I. Einleitung

Zum Stichtag 31.12.2015 waren in Österreich rund 4,75 Mio. Pkw zugelassen[1]. Wie viele davon Smart Cars, „connected cars", „vernetzte Fahrzeuge", „intelligente Fahrzeuge" sind ist schwer abzuschätzen. Die erste Frage die man sich dazu stellen muss ist, was macht ein Fahrzeug überhaupt „smart"? Ist das schon ein Fahrzeug mit Anti Blockier System (ABS)? Mit Elektronischem Stabilitätsprogramm (ESP)? Oder vielleicht doch erst wenn es über Mobilfunk, WLAN oder andere Kommunikationstechniken einen Zugang zum Internet herstellt? Smart Cars sind eine Weiterentwicklung des „Mobile Computing" das erst vor ein paar Jahren den Durchbruch mit internetfähigen Smartphones erlebt hat[2] und sich weiter fortgesetzt hat mit „smart glasses", „smart watches" und eben auch mit Smart Cars. Das Internet of Things (IoT), also die Vernetzung von Gegenständen damit diese „smart" werden, ist die Zukunft. Die Systeme der Fahrzeuge werden immer öfters mit einer eigenen SIM-Karte ausgestattet, um sich über das Internet mit verschiedenen Services und mit den Servern des Herstellers verbinden zu können um z.B. Updates over-the-air herunterzuladen und einzuspielen. Auch die Mobilfunkprovider haben diesen Trend und dieses Geschäftsfeld erkannt und bieten für solche Zwecke spezielle Tarife für Fahrzeughersteller unter dem Schlagwort M2M[3] an.

Die modernen Fahrzeuge sind immer mehr auch direkt mit anderen Fahrzeugen, der Infrastruktur und der Umwelt verbunden (C2C, C2X). Ein Beispiel dafür ist die digitale Vignette[4]. Dadurch soll die Verkehrssicherheit, das Fahrerlebnis und der Komfort verbessert werden. Die Fahrer sollen durch aktuelle Informationen (Verkehrsaufkommen, Stau, Unfall) schneller an ihr Ziel kommen und dadurch das Autofahren komfortabler und sicherer werden. Autos haben heute eine Vielzahl von Sensoren (z.B. Positions- (=GPS), Raddrehzahl-, Regen-, Video und Ultraschallsensoren) und speichern dadurch auch eine Vielzahl anderer

---

[1] *Statistik Austria*, Kfz-Bestand 2015 <http://www.statistik.at/wcm/idc/idcplg?IdcService=GET_PDF_FILE&RevisionSelectionMethod=LatestReleased&dDocName=107010>.

[2] *Weichert*, Datenschutz im Auto, Das Kfz als großes Smartphone mit Rädern, SVR 2014, 201.

[3] *Weisser/Färber*, Rechtliche Rahmenbedingungen bei Connected Cars – Überblick über die Rechtsprobleme der automobilen Zukunft, MMR 2016 507.

[4] *Asfinag* <http://www.asfinag.at/maut/vignette/digitale_vignette>.

Daten (z.B. Sitzposition, wie oft ein physisches Medium im entertainment center verwendet wurde, wie viele Personen sich im Auto befinden).

Die Daten, die dabei entstehen haben auch einen Wert. Wie wichtig und wertvoll zum Beispiel Kartendaten sind, hat sich bei einer Versteigerung des Kartendienstes „Nokia Here" 2015 gezeigt, wo der Kartendienst für 2,8 Milliarden Euro von einem Konsortium mehrerer Autohersteller ersteigert wurde als Antwort auf „Apple CarPlay[5]" und „Android Auto[6]" die als Betriebssystem (Boardsystem) für Fahrzeuge antreten und ebenfalls Kartendienste und andere Features (smartphone applications, Appstores) anbieten.

Diese „Intelligenz" hat viele Vorteile und kann durch die vielen Sicherheitsanwendungen Leben retten. Beispiele dafür sind der Lenk- und Spurführungsassistent, Abstandsassistent und viele mehr. Durch die Verpflichtung der Autohersteller Neufahrzeuge ab 31. März 2018 mit eCall[7] auszustatten, wird bei einem Unfall sogar vom Fahrzeug selbst ein Notruf abgeschickt, welcher auch gleich die Position des Fahrzeugs beinhaltet (daneben auch noch andere essentielle Daten, Stichwort MSD[8]).

Versicherungsunternehmen bieten auch immer öfters Versicherungen an, wo für die Berechnung der KFZ-Versicherungsprämie das Fahrverhalten des Versicherungsnehmers herangezogen wird (Pay-As-You-Drive). Bei dieser Art von Versicherung werden die Fahrdaten des Versicherungsnehmers mittels einer OBU (On Board Unit) gesammelt und ausgewertet. Nach Auswertung der Daten kann die Versicherung bei aggressivem Fahren die Prämien erhöhen, aber bei defensivem Fahren die Prämien senken. Die österreichischen Versicherer haben für Pay-As-You-Drive allerdings eine distanzabhängige und nicht eine auf das Fahrverhalten abzielende Prämienberechnung herangezogen. Fährt man also weniger als z.B. 5000 km pro Jahr, spart man sich einen Teil der Prämie[9].

Mit dieser Arbeit möchte ich untersuchen, welche Daten von den Fahrzeugen gesammelt werden, wie dies datenschutzrechtlich zu beurteilen ist und einen Ausblick auf die kommende Datenschutz Grundverordnung geben.

---

[5] *Apple Inc.* <http://www.apple.com/ios/carplay/>.

[6] *Google Inc.* <https://www.android.com/auto/>.

[7] Verordnung 2015/758 des europäischen Parlaments und des Rates vom 29. April 2015 über Anforderungen für die Typgenehmigung zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG.

[8] EN 15722:2011, "Intelligente Transportsysteme - Elektronische Sicherheit - Minimaler Datensatz (MSD) für den elektronischen Notruf eCall".

[9] *Brandl/Paffeneder*, Datenschutzrechtliche Aspekte der Pay-As-You-Drive Versicherung, in Jahnel (Hrsg), Datenschutzrecht. Jahrbuch 2014 (2014) 191; *Allianz*, Besondere Bedingung Pay As You Drive (PAYD) – „Fahr und Spar" – Tarif <https://www.allianz.at/v_1438676973000/firmenkunden/produkte/dokumente/BesBed_Fahr_und_Spar.pdf >.

II. Technische Grundlagen

A. Welche Daten fallen an?

Smart Cars sind eine Kombination aus Hardware und Software. Die Hardware setzt sich aus unterschiedlichen Sensoren zusammen, diese Sensoren erzeugen Datensätze, die mit Hilfe der Software ausgewertet und gegebenenfalls dargestellt und übermittelt werden. Diese gesammelten Daten werden als Mobilitätsdaten bezeichnet.

Im Jahr 2015 wurde vom ADAC im Auftrag der FIA eine Studie mit dem Titel „MyCarMyData" durchgeführt, die sich mit dem Thema Datenverarbeitung und Datenübermittlung von Fahrzeugdaten auseinander setzte. Im Lauf dieser Studie konnte ermittelt werden welche Anzahl und Art von Daten verarbeitet und gespeichert wurde. Es konnte jedoch nicht festgestellt werden, welche Daten davon auch zu dem Hersteller übertragen werden. Die Bandbreite der verarbeiteten Daten reicht von 10 GB[10] pro Stunde bis 25 GB[11] pro Stunde. Ein Hersteller behauptet, dass davon nur 20-30 Mbyte[12] pro Monat übertragen werden[13].

Die ermittelten (Mobilitäts-)Daten können in zwei Gruppen eingeteilt werden:

Einerseits in Daten die sich auf das Fahrzeug selbst beziehen und in Daten die bei der Fahrt anfallen, so genannte Telematikdaten.

Fahrzeugdaten sind unter anderem[14]:

- die Fahrzeug-Identifizierungsnummer (Vehicle Identification Number (VIN))
- MAC-Adresse (Media Access Control) der Netzwerkkarte für die Kommunikation mit WLAN (Wireless Local Area Network)
- RFID-Kennung bei Schlüsseln
- IP-Adresse
- Die Nummer der SIM-Karten (Subscriber Identity Module) für die Datenübertragung oder Telefonie
- Daten über die Gangschaltung (wie lange welcher Gang verwendet wurde)

---

[10] *Stepanek*: „Jedes Auto produziert 10 GB Daten pro Stunde", Futurezone, 29.04.2013, <http://futurezone.at/science/jedes-auto-produziert-10-gb-daten-pro-stunde/24.595.665>.

[11] *Hitachi Data Systems*, The Internet on Wheels and Hitachi, Ltd. White Paper, November 2014, <http://www.hds.com/assets/pdf/hitachi-white-paper-internet-on-wheels.pdf>.

[12] *Golem*, ADAC fordert Ausschaltknopf für Datentransfers, <http://www.golem.de/news/vernetztes-fahren-adac-fordert-ausschaltknopf-fuer-datentransfers-1602-119372-2.html>.

[13] *Golem*, Wie mit Fantasiezahlen Politik gemacht wird <http://www.golem.de/news/vernetztes-fahren-wie-mit-fantasiezahlen-politik-gemacht-wird-1603-119485.html>.

[14] *Hansen*, Das Netz im Auto & das Auto im Netz, DuD 2015, 367.; *FIA Federation Internationale de l'Automobile*, Technical Study, MyCarMyData, 8.

- Daten über die Sitze (wie lange die Sitzheizung verwendet wurde, Einstellposition des Sitzes, Anzahl der Personen im Fahrzeug)
- Daten über die Beleuchtung (wie lange die Scheinwerfer in Betrieb waren)
- Daten über den Sicherheitsgurt (wie oft der Sitzgurt gestrafft wurde aufgrund einer Bremsung)

Zu Telematikdaten gehören z.B.:

- Standortdaten über GPS (Global Positioning Service), Mobilfunkzellen, WLAN access points
- Geschwindigkeit
- Fahrtrichtung

Daneben kann auch noch ein Unfalldatenspeicher (Event Data Recorder (EDR)) verbaut sein, welcher die Daten der Sensoren zur Messung von Beschleunigung, Geschwindigkeit, Verwendung der Bremse, etc. bei einem Unfall speichert und damit eine Blackbox ähnliche Funktion erfüllt. Die gespeicherten Daten können im Anschluss von Sachverständigen und der Werkstatt zur Rekonstruktion des Unfalles herangezogen werden[15].

B. Wie werden diese Daten übertragen?

Die Übertragung der Daten ist auf mehreren Wegen möglich. Eine Möglichkeit ist die Übertragung sobald das Fahrzeug in einer Werkstatt mit einem Diagnosegerät verbunden wird. Hierbei können die Fahrzeugdaten ausgelesen werden und an die Server des Herstellers z.B. zur Qualitätssicherung und Überprüfung etwaiger Manipulationen wie Tuning oder Änderung am Hauptrechner, übermittelt werden[16]. Da ein Werkstattbesuch im Regelfall nur 1-2-mal pro Jahr erfolgt, sind bei dieser Art der Übertragung, große Datensätze vorhanden, die zwischen den Besuchen entstanden sind und daher ein genaues Profil des Fahrers zeichnen können. Aus diesen (Positions-)Daten ist dann jedenfalls ersichtlich, wo der Fahrer wohnt, arbeitet und seine Freizeit verbringt.

Eine weitere Möglichkeit ist die Übertragung der Daten zwischen zwei Fahrzeugen. Bei der Car2Car Kommunikation (C2C)[17] kommunizieren Fahrzeuge nicht über einen Server sondern unmittelbar miteinander. Fahrzeuge können sich so gegenseitig über Staus, Verkehrsunfälle,

---

[15] *FIA Federation Internationale de l'Automobile*, Technical Study, MyCarMyData, 7.

[16] *FIA Federation Internationale de l'Automobile*, Technical Study, MyCarMyData, 8.

[17] Im englischsprachigen Raum als V2V Vehicle to Vehicle bezeichnet.

Glatteis oder ähnliche Gefahrenstellen informieren und vorwarnen. Die Kommunikation zwischen den Fahrzeugen erfolgt durch die Verwendung von funkbasierten Verfahren wie GSM/UMTS/LTE, Bluetooth oder WLAN[18]. Die Kommunikation kann auch über weite Strecken erfolgen, da die Daten von Fahrzeug zu Fahrzeug weitergeleitet werden können. Daneben gibt es noch Car2X (C2X)[19] welcher als Oberbegriff mehrere Techniken zusammenfasst bei denen das Fahrzeug mit einer anderen Einheit kommuniziert wie z.B. Car to Infrastructure[20], Car to Pedestrian[21], Car to Grid[22](C2I, C2P, C2G)[23].

Möglich ist auch eine Übermittlung der Daten über ein Mobilfunknetz, da die meisten Neufahrzeuge bereits eine SIM-Karte integriert haben und durch die Verpflichtung von eCall ab 2018, alle Neufahrzeuge haben werden. Die Fahrzeuge können dann die entstandenen Daten, in Echtzeit, an die Server des Fahrzeugherstellers übermitteln und diese werden anschließend im Rechenzentrum ausgewertet. Möglich wäre auch eine Übertragung bei bestimmten Zeitpunkten (nach Fahrtende[24], bei Fahrerwechsel, wöchentlich, monatlich) oder bei bestimmten Ereignissen (Unfall, scharfe Bremsung, überhöhte Geschwindigkeit)[25].

III. Datenschutz

Die Grundstruktur des österreichischen Datenschutzrechtes besteht aus drei Ebenen[26]:

- europäische Ebene
- nationales Recht im Verfassungsrang
- einfachgesetzliche Rechtsgrundlagen

---

[18] *Horz*, Car2Car Kommunikation, 3. < https://www.uni-koblenz-landau.de/de/koblenz/fb4/ist/AGZoebel/Lehre/sommer2013/SeminarASidA/Horzz>; *Weisser/Färber*: Rechtliche Rahmenbedingungen bei Connected Car Überblick über die Rechtsprobleme der automobilen Zukunft, MMR 2015, 507.

[19] Im englischsprachigen Raum als V2V Vehicle to X bezeichnet.

[20] z.B. für gesteuerte Ampelanlagen oder Mautsysteme.

[21] *Engadget*,<http://www.engadget.com/2016/02/08/smart-car-algorithm-sees-pedestrians-as-well-as-you-can>.

[22] Fahrzeuge können als intelligente Zwischenspeicher für das Stromnetz verwendet werden siehe *Heuer*, Rollende Kraftwerke, Technology Review, 104. <http://www.udel.edu/V2G/docs/Heuer-TechReviewV2G-04.pdf>.

[23] *IT-Wissen*, Das große Online-Lexikon für Informationstechnologie <http://www.itwissen.info/definition/lexikon/V2X-vehicle-to-x.html >.

[24] *FIA Federation Internationale de l'Automobile*, Technical Study, MyCarMyData, 8.

[25] *Brandl/Paffeneder*, Datenschutzrechtliche Aspekte der Pay-As-You-Drive Versicherung, in Jahnel (Hrsg), Datenschutzrecht. Jahrbuch 2014 (2014) 205.

[26] *Jahnel*, Datenschutzrecht, Rz 1/20.

A. Datenschutz auf europäischer Ebene

Auf europäischer Ebene gibt es die Richtlinie 95/46/EG[27], welche 2018 durch die Datenschutz Grundverordnung ersetzt wird und in Österreich mit dem DSG 2000 umgesetzt wurde, sowie die Richtlinie 2002/58/EG[28], welche die allgemeine Datenschutzrichtlinie sektorspezifisch für elektronische Kommunikation ergänzt.

Des Weiteren den Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, welche den Datenschutz für den Polizei- und Justizsektor sektoral regelt und ebenfalls 2018 durch eine Richtlinie ersetzt wird.

Erwähnenswert ist auch noch die Europarats-Konvention ETS 108 („Datenschutz-Konvention“). Bei der Konvention handelt es sich um einen multilateralen Staatsvertrag, der bisher das einzige multilaterale Instrument ist, welches Datenschutz zum Gegenstand hat. Eine Ratifizierung ist auch durch außereuropäische Staaten möglich (bis jetzt ratifiziert von Uruguay). Die Konvention regelt die wichtigsten Punkte des Datenschutzrechtes und wird ebenfalls derzeit einer Novellierung unterzogen.

B. DSG 2000

Auf nationaler Ebene gibt es das DSG 2000, welches aus 2 Artikeln besteht, wobei Artikel 1 im Verfassungsrang steht und Artikel 2 alle anderen (einfachgesetzlichen) Bestimmungen beinhaltet. Artikel 1 § 1 DSG 2000 gewährt das Grundrecht auf Datenschutz und beinhaltet das Recht auf Geheimhaltung personenbezogener Daten (§ 1 Abs 1 DSG 2000), Recht auf Auskunft (§ 1 Abs 3 Z 1 DSG 2000), Recht auf Richtigstellung unrichtiger Daten (§ 1 Abs 3 Z 2 DSG 2000) und das Recht auf Löschung unzulässigerweise verarbeiteter Daten (§ 1 Abs 3 Z 2 DSG 2000).

Das Grundrecht auf Geheimhaltung ist sehr weit und erfasst personenbezogene Daten, soweit daran ein schutzwürdiges Interesse besteht. Hierbei kann es sich auch um manuell verarbeitete Daten handeln (im Gegensatz zu § 1 Abs 3 DSG 2000). Bei den Begleitrechten (Recht auf Auskunft, Richtigstellung oder Löschung) muss es sich um Daten handeln, die automationsunterstützt verarbeitet werden oder zur Verarbeitung in einer manuellen Datei

---

[27] Richtlinie 95/46/EG des europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[28] Richtlinie 2002/58/EG des europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

geführt werden[29]. Automationsunterstützt bedeutet eine Verarbeitung der Daten unter Einsatz von EDV[30]. Grundrechtsträger ist Jedermann. In Österreich betrifft dies nicht nur natürliche sondern auch juristische Personen[31] und ist nicht an den Besitz der österreichischen Staatsbürgerschaft[32] gebunden. Das Grundrecht besteht nur dann, wenn es sich um personenbezogene Daten handelt und ein schutzwürdiges Geheimhaltungsinteresse daran besteht. Dieses besteht nicht, wenn die Daten allgemein verfügbar oder nicht auf eine Person rückführbar (anonym) sind. Allgemein verfügbar bedeutet, dass die Daten öffentlich sind (z.B. Telefonbuch) oder durch Auslegung des § 8 Abs 2 DSG 2000 zulässigerweise veröffentlicht wurden. Dies sind unter anderem Daten aus dem Grundbuch, Firmenbuch, Datenverarbeitungsregister aber auch im Internet publizierte Daten[33]. Die Daten, die bei einem Smart Car anfallen, sind nicht allgemein verfügbar. Des Weiteren sind sie, zumindest über den Fahrzeughalter, auf eine Person rückführbar. Es besteht daher ein schutzwürdiges Geheimhaltungsinteresse an den Mobilitätsdaten. Der Betroffene hat einen Anspruch auf Geheimhaltung seiner Verbrauchsdaten gemäß § 1 Abs 1 DSG 2000.

Der Anwendungsbereich des DSG 2000 ist in den §§ 2 und 3 geregelt. Der Bund hat die Kompetenz in Gesetzgebung und Vollziehung in Angelegenheiten des Schutzes personenbezogener Daten im automationsunterstützten Datenverkehr[34]. Daraus folgt, dass für manuelle Dateien grundsätzlich die Gesetzgebungskompetenz jener Gebietskörperschaft, die für die gesetzliche Regelung des Zwecks, dem die Datenverwendung dienen soll, (Annexmaterie) zuständig ist[35]. § 3 DSG 2000 besagt, dass grundsätzlich das DSG 2000 auf jede Datenanwendung in Österreich anzuwenden ist. Durchbrochen wird diese Regel vom Sitzstaatprinzip. Es wird für eine Datenanwendung dann das Recht des Sitzstaates angewendet, wenn Daten in Österreich für einen Auftraggeber des privaten Bereichs aus einem anderen EU Staat verarbeitet werden, ohne dass der Auftraggeber eine Niederlassung hat[36]. Ist der Sitz außerhalb der EU, ist der Ort der Datenverarbeitung maßgeblich. Die Verarbeitung von Daten in einem Smart Car erfolgt automationsunterstützt und in Österreich, daher ist das DSG 2000 anwendbar.

---

[29] *Jahnel*, Datenschutzrecht in der Praxis, 12.

[30] *Jahnel*, Datenschutzrecht, Rz 2/30.

[31] *Jahnel*, Datenschutzrecht in der Praxis, 14.

[32] *Jahnel*, Datenschutzrecht, Rz 2/4.

[33] *Knyrim*, Datenschutzrecht3, 114.

[34] § 2 Abs 1 DSG 2000.

[35] *Jahnel*, Datenschutzrecht, Rz 3/2.

[36] *Unger*, Grundzüge des Datenschutzrechts[2],4.; *Jahnel*, Datenschutzrecht in der Praxis, 14.

Begriffsbestimmungen

a) Personenbezogene Daten

Personenbezogene Daten[37] sind Angaben über Betroffene (natürliche oder juristische Personen), deren Identität bestimmt oder bestimmbar ist (§ 4 Abs 1 DSG 2000). Der Begriff „Angaben" umfasst unter anderem Name, Geburtsdatum, Adresse, E-Mail Adresse, Geschlecht, Körpermerkmale, Biometrische Daten (Fingerabdruck, Iris-Muster), ZMR-Nummer, Kundennummer. Zu personenbezogenen Daten zählen aber auch Standortdaten (GPS, Mobiltelefon), Konsum-, Zahlungs- und Freizeitverhalten, Einkommen oder Vermögen. Auch Werturteile und Vermutungen, egal ob wahr oder falsch, gelten als personenbezogene Daten[38]. Ist die Identität nicht direkt ersichtlich, sondern kann diese erst mit Zusatzinformationen festgestellt werden, spricht man von Bestimmbarkeit[39].

Mobilitätsdaten beziehen sich nicht zwangsläufig auf eine bestimmte Person, jedenfalls aber auf ein bestimmtes Fahrzeug[40]. Da ein Fahrzeug aber einem Halter zugerechnet werden kann, wird in der Literatur vertreten, dass der Fahrer für einen Personenbezug mit ausreichend hoher Wahrscheinlichkeit bestimmbar ist und es sich daher um personenbezogene Daten handelt[41]. Bei einem Smart Car kann sich der Personenbezug aus mehreren Daten ergeben. Einerseits können dies Geräte-IDs, MAC-Adresse der Netzwerkkarte (kann nicht geändert werden), IP-Adresse, IMSI (eindeutige Kennung der SIM-Karte im Netz) aber auch Merkmalskombinationen daraus sein. So wie ein Browser-Fingerprint zum tracken verwendet wird, ist wohl auch das tracken eines Fahrers über die Telematikdaten möglich. Kommen auch noch Standortdaten dazu, kann ein Profil des Fahrers erstellt werden, aus dem ersichtlich ist, wo diese Person wohnt, arbeitet und die Freizeit verbringt. Mobilitätsdaten sind daher jedenfalls personenbezogene Daten und das DSG 2000 daher anwendbar.

b) Sensible Daten

Sensible Daten sind Daten natürlicher Personen, über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung,

---

[37] Siehe auch *Art-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, 01248/07/DE, <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf>.

[38] *Jahnel*, Datenschutzrecht, Rz 3/72; *Dohr/Pollirer/Weiss/Knyrim*, DSG 2000. Datenschutz2§ 4 Anm 2.

[39] *Jahnel*, Datenschutzrecht, Rz 3/76.

[40] *Pachinger*, Datenschutzrechtliche Fragen zu Mobilitätsdaten, ZIIR 2015, 266.

[41] *Brandl/Paffeneder*, Datenschutzrechtliche Aspekte der Pay-As-You-Drive Versicherung, in Jahnel (Hrsg), Datenschutzrecht. Jahrbuch 2014 (2014) 191; siehe auch Art 29 Datenschutzgruppe WP 188 zur Auswertung von Cookie Daten und IP Adressen.

Gesundheit oder ihr Sexualleben (§ 4 Z 2 DSG 2000). Diese Aufzählung ist taxativ und darf weder erweitert noch verkürzt werden[42].

Weder Mobilitätsdaten als gesamtes Datenpaket, noch die in II. A. genannten einzelnen Daten, sind sensible Daten im Sinn des § 4 Z 2 DSG 2000 da, diese taxativ aufgezählt sind und Mobilitätsdaten nicht unter einen dieser Begriffe subsumiert werden können. Möglich ist aber, dass es sich dabei um potentiell sensible Daten handeln könnte, wo erst ersichtlich ist dass es sich um sensible Daten handelt, nachdem man diese ausgewertet hat. Durch Auswertung der Positionsdaten kann ein einstündiger Aufenthaltsort in der Nähe einer Kirche, eines Arztes oder Spitals, die Teilnahme an einer Demonstration oder die Nähe zu einem Bordell, ein sensibles Datum sein[43]. Dass Rückschlüsse auf eine einzelne Person möglich sind, wenn es mehrere Fahrer geben sollte, ist aber eher unwahrscheinlich.

c) Auftraggeber

Auftraggeber („für die Verarbeitung Verantwortlicher" nach der Diktion der RL 95/46/EG und der DS-GVO) ist nach § 4 Z 4 DSG 2000 jede natürliche oder juristische Person, Personengemeinschaft oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten zu verwenden, unabhängig davon, ob sie die Daten selbst verwenden oder damit einen Dienstleister beauftragen. Sie gelten auch dann als Auftraggeber, wenn der mit der Herstellung eines Werkes beauftragte Dienstleister, die Entscheidung trifft, zu diesem Zweck Daten zu verwenden, es sei denn dies wurde ihm ausdrücklich untersagt oder der Beauftragte hat auf Grund von Rechtsvorschriften oder Verhaltensregeln über die Verwendung eigenverantwortlich zu entscheiden. Den Auftraggeber trifft die Verantwortung der Datenverarbeitung. Er muss sich um die Einhaltung des Datenschutzgesetzes kümmern und hat alle Vorkehrungen zu treffen damit die Daten sicher sind[44].

Im Fall der Smart Cars ist zu prüfen wer Träger der Auftraggebereigenschaft sein kann. In der Entscheidung K121.245/0009-DSK/2007 hat die Datenschutzkommission festgestellt, dass die Auftraggebereigenschaft „die Folge eines faktischen Verhaltens, nämlich einer autonom getroffenen Entscheidung, bestimmte Verarbeitungsschritte zu setzen" ist. Aufgrund dieser Definition kann der Hersteller, der Dienstleister, aber auch der Fahrer, Auftraggeber sein. Der Fahrer indem er z.B. die Kontakte von seinem Mobiltelefon mit dem Fahrzeug synchronisiert,

---

[42] *Dohr/Pollirer/Weiss/Knyrim*, DSG 2000. Datenschutz[2], 62.

[43] *Bundesministerium für Verkehr, Innovation und Technologie*, Handbuch für Mobilitätserhebungen: KOMOD - Konzeptstudie Mobilitätsdaten Österreichs, 101.

[44] *Unger*, Grundzüge des Datenschutzrechts[2], 9; *Knyrim*, Datenschutzrecht3, 41.

der Dienstleister der seine Navigationssoftware anbietet und der Hersteller, welcher das Fahrzeug als „Komplettpaket“ anbietet. Die Auftraggebereigenschaft des Herstellers beginnt aber erst, wenn das Fahrzeug von dem Käufer in Betrieb genommen wird, da erst dann ein personenbezogenes Datum vorliegt[45]. Es dürfte unbestritten sein, dass dem Hersteller, abhängig von der Datenverwerwendung, die Gesamtverantwortung zukommt, da sich dieser auch entscheidet, welche Hardware und welche Software mit welchen Funktionen ausgeliefert wird[46] und somit „Herr der Daten“[47] ist.

d) Dienstleister

Der Dienstleisterbegriff ist in § 4 Z 5 DSG 2000 definiert. Demnach ist ein Dienstleister eine natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden (= verarbeiten und übermitteln). Gemeint sind damit primär Gewerbetreibende, die Dienstleistungen iSd § 153 GewO erbringen (Gewerbetreibende, die zur Ausübung des Gewerbes der Dienstleistungen in der automatischen Datenverarbeitung und Informationstechnik berechtigt sind)[48]. Der Dienstleister kann aber auch zum Auftraggeber iSd § 4 Z 4 DSG 2000 werden, wenn er die Daten, anders oder gegen den Auftrag des Auftraggebers verwendet, Daten mehrerer Auftraggeber verknüpft, aber auch, wenn ein Werk mit Daten, die gegen Entgelt erworben wurden, hergestellt wird[49]. Die Pflichten des Dienstleisters sind in § 11 DSG 2000 definiert. In der DSRL und der DS-GVO wird von einem Auftragsverarbeiter gesprochen.

Dienstleister im Bereich des Smart Car können Unternehmen sein, welche eine technische Infrastruktur für den Transport und Speicherung der Daten in einem Rechenzentrum zur Verfügung stellen.

e) Betroffener

Betroffener ist jede natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet und vom Auftraggeber verschieden ist (§ 4 Z 3 DSG 2000). Der Begriff „Betroffene“ wurde aus dem DSG 1978 übernommen.

---

[45] DSK 26.09.2006, K121.150/0014-DSK/2006 = MR 2006, 344 (*Steiner*).

[46] *Weichert*, Datenschutz im Auto, SVR 2014, 205.

[47] *Dohr/Pollirer/Weiss/Knyrim*, DSG 2000. Datenschutz[2], 71.

[48] *Dohr/Pollirer/Weiss/Knyrim*, DSG 2000. Datenschutz[2], 72/1.

[49] *Jahnel*, Datenschutzrecht, Rz 3/48; *Unger*, Grundzüge des Datenschutzrechts[2],9.; *Knyrim*, Datenschutzrecht[3], 12.

Betroffener kann daher der Fahrer bzw. Beifahrer, der Halter aber auch andere Verkehrsteilnehmer sein. Andere Verkehrsteilnehmer als Betroffene sind heutzutage eher unwesentlich. Durch die zunehmende Automatisierung wird sich dies aber künftig ändern, da immer mehr Fahrzeuge miteinander kommunizieren (C2C)[50].

C. TKG als lex specialis

Wie schon bei den Grundlagen des Datenschutzes auf europäischer Ebene erwähnt, wird die allgemeine Datenschutzrichtlinie (RL 95/46/EG) sektorspezifisch für elektronische Kommunikation ergänzt. Das Internet eröffnet neue Chancen und Möglichkeiten, schafft aber gleichzeitig auch Risiken in Bezug auf die personenbezogenen Daten und die Privatsphäre des Nutzers[51]. Für öffentliche Kommunikationsnetze sollen daher besondere rechtliche, und technische Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen erlassen werden, da die Möglichkeiten und Fähigkeiten zur automatischen Speicherung und Verarbeitung personenbezogener Daten immer größer werden[52]. Die allgemeine Datenschutzrichtlinie (RL 95/46/EG) gilt im Bereich der elektronischen Kommunikation vor allem für Fragen des Schutzes der Grundrechte und Grundfreiheiten, die von der Richtlinie für elektronische Kommunikation nicht erfasst werden und ist anwendbar bei nicht öffentlichen Kommunikationsdiensten[53].

National wurde die Richtlinie für elektronische Kommunikation mit dem TKG 2003[54] umgesetzt. Das allgemeine Datenschutzrecht ist also im DSG 2000 geregelt und wird sektoral durch die Datenschutzbestimmungen für die elektronische Kommunikation im TKG 2003 ergänzt[55]. Zu prüfen ist nun, ob die besonderen Datenschutzbestimmungen auf Smart Cars anzuwenden sind, da Daten über ein öffentliches Kommunikationsnetz übermittelt werden (integrierte SIM-Karte in dem Fahrzeug für z.B. einen Notruf).

Der 12. Abschnitt des TKG 2003 („Kommunikationsgeheimnis, Datenschutz“) ist anzuwenden bei der Verarbeitung und Übermittlung von personenbezogenen Daten, in Verbindung mit der Bereitstellung öffentlicher Kommunikationsdienste in öffentlichen Kommunikationsnetzen[56]. Die Begriffsbestimmungen eines Kommunikationsdienstes und die

---

[50] *Weichert*, Datenschutz im Auto, Das Kfz als großes Smartphone mit Rädern, SVR 2014, 204.

[51] ErwGr 6 RL 2002/58/EG.

[52] ErwGr 7 RL 2002/58/EG.

[53] ErwGr 10 RL 2002/58/EG.

[54] Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003), BGBl. I Nr. 70/2003.

[55] *Stratil* (Hrsg), TKG 2003[4] § 92 Anm 3 (2013).

[56] § 92 Abs 1 TKG 2003.

eines öffentlichen Kommunikationsnetzes, befinden sich in § 3 TKG 2003. Demnach ist ein „Kommunikationsdienst“[57] eine gewerbliche Dienstleistung, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze besteht. Der Begriff „öffentlicher Kommunikationsdienst“ ist nicht definiert, jedoch findet sich im § 3 Z 17 TKG 2003 die Definition eines „öffentlichen Kommunikationsnetzes“. Dieses ist ein Kommunikationsnetz, das ganz oder überwiegend zur Bereitstellung öffentlich zugänglicher Kommunikationsdienste dient.

Wie oben ausführlich dargelegt, werden von Smart Cars personenbezogene Daten verarbeitet. Diese Verarbeitung und Übermittlung muss aber, damit die lex specialis des TKG 2003 anzuwenden ist, in Verbindung mit der Bereitstellung öffentlicher Kommunikationsdienste in öffentlichen Kommunikationsnetzen passieren. In der Literatur wird sowohl im Bereich der Pay-As-You-Drive Versicherungen[58] als auch für die Datenverarbeitung im Bereich eCall[59] vertreten, dass weder der eCall-Dienst noch die Übertragung der Standortdaten durch den Versicherer als Kommunikationsdienst im Sinn des § 3 Z 9 TKG 2003 zu qualifizieren ist, da keine Dienstleistung erbracht wird, die ganz oder überwiegend in der Übertragung von Signalen besteht[60].

Dies trifft meiner Meinung nach auch für die Datenverarbeitung in Smart Cars zu, da auch hier keine eigene Dienstleistung erbracht wird, die ganz oder überwiegend in der Übertragung von Signalen besteht. Das öffentliche Kommunikationsnetz wird für die Datenübertragung nur als Vehikel zwischen dem Fahrzeug und den Servern des Fahrzeugherstellers genutzt[61]. Die Dienstleistungen bei einem Smart Car sind unter anderem aktuelle Navigationsdaten, Services wie „find my car“, wenn man sich nicht mehr erinnern kann, wo man das Auto zuletzt geparkt hat, oder auch eCall. Selbst wenn Internet über ein öffentliches Kommunikationsnetz als Dienstleistung angeboten wird, wäre dies nur eine Dienstleistung neben vielen anderen[62]. Die Anwendbarkeit des TKG 2003 als lex specialis zu den Bestimmungen des DSG 2000 ist daher zu verneinen.

---

[57] § 3 Z 9 TKG 2003.

[58] *Brandl/Paffeneder*, Datenschutzrechtliche Aspekte der Pay-As-You-Drive Versicherung, in Jahnel (Hrsg), Datenschutzrecht. Jahrbuch 2014 (2014) 205.

[59] *Pachinger*, Datenschutzrechtliche Fragen zu Mobilitätsdaten, ZIIR 2015, 268.

[60] Anderer Meinung ist das Verwaltungsgericht Köln, 11.11.2015, 21 K 450/15 welches Gmail (E-Mail Programm von Google) als einen Telekommunikationsdienst definierte.

[61] *Weisser/Färber*: Rechtliche Rahmenbedingungen bei Connected Car Überblick über die Rechtsprobleme der automobilen Zukunft, MMR 2015, 509.

[62] *Stratil* (Hrsg), TKG 2003[4] ErläutRV zu § 3 Z 9 TKG 2003.

D. Datenschutz Grundverordnung (DS-GVO)

Um den Datenschutz in Europa zu stärken und die Wirtschaft Europas anzukurbeln, hat die europäische Kommission eine Reform des Datenschutzrechts vorgeschlagen. Die Datenschutzreform ist ein „Datenschutzpaket", welches aus zwei Teilen besteht: Der erste Teil beinhaltet die Datenschutz Grundverordnung, welche die Grundlage eines einheitlichen Datenschutzes in Europa sein wird und die die RL 95/46/EG ersetzt und der zweite Teil beinhaltet die Richtlinie für den Bereich Justiz und Inneres, welche den bisherigen Rahmenbeschluss ersetzt[63]. Ziel der Reform ist eine Modernisierung und Aktualisierung des Datenschutzrechtes. Um dieses Ziel zu erreichen ist eine einheitliche und aktuelle Datenschutzgesetzgebung notwendig, um den grundrechtlichen Schutz personenbezogener Daten zu garantieren, technologische Entwicklungen zu ermöglichen und die Bekämpfung von Kriminalität und Terrorismus zu verstärken[64]. Eine politische Einigung über den Inhalt, wurde im Dezember 2015 erzielt. Offizielle Übersetzungen in alle Amtssprachen werden im ersten Halbjahr 2016 erwartet. Anwendbar wird die DS-GVO zwei Jahre nach Veröffentlichung (2018). Bei der DS-GVO handelt es sich um eine „hinkende Verordnung", da innerstaatlich Umsetzungsmaßnahmen notwendig sind (z.B. Datenschutzbehörde, Arbeitnehmerdaten, Freiheit der Meinungsäußerung).

Begriffsbestimmungen

a) Personenbezogene Daten

Die DS-GVO bringt bei der Definition von personenbezogenen Daten keine wesentlichen Neuerungen. Wie auch schon in der RL 95/46/EG, umfasst auch die DS-GVO nur Daten natürlicher Personen aber keine juristischen Personen[65]. Eine Aufrechterhaltung des Schutzes für juristische Personen erscheint mE möglich aufgrund von Öffnungsklauseln und dass eine juristische Person als Betroffener nicht ausgeschlossen ist, wäre aber fragwürdig, da das Ziel der DS-GVO eine Vereinheitlichung des Datenschutzes in Europa anstrebt und Österreich als eines von wenigen Staaten diesen Schutz gewähren würde.

---

63 Rahmenbeschluss 2008/977/JI des Rates der Europäischen Union vom 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.

64 *Europäischer Rat zur Datenschutzreform* <http://www.consilium.europa.eu/de/policies/data-protection-reform/>.

65 *Dörnhöfer*, Datenschutz bei Grenzüberschreitungen. Zur Anwendbarkeit des DSG 2000 in grenzüberschreitenden Konstellationen, in Jahnel (Hrsg), Datenschutzrecht und E-Government. Jahrbuch 2012 (2012) 59.

Im Ergebnis kann auf die Ausführung im Abschnitt personenbezogene Daten nach dem DSG 2000 verwiesen werden.

b) Sensible Daten

Sensible Daten sind nach der DS-GVO Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer Person oder Daten über Gesundheit oder Sexualleben und sexuelle Ausrichtung (Art. 9 DS-GVO). Diese Aufzählung ist taxativ und inkludiert nun auch, im Gegensatz zur RL 95/46/EG und dem DSG 2000, die sexuelle Orientierung, genetische- und biometrische Daten.

Auch hier kann im Ergebnis auf die Ausführungen, im Abschnitt sensible Daten, nach dem DSG 2000, verwiesen werden, da auch der Katalog, nach der DS-GVO, taxativ ist und Mobilitätsdaten sich nicht darunter subsumieren lassen.

c) Für die Verarbeitung Verantwortlicher

Nach der DS-GVO Artikel 4 ist ein "für die Verarbeitung Verantwortlicher" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der für die Verarbeitung Verantwortliche beziehungsweise die Modalitäten seiner Benennung, nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, bestimmt werden.

Hier gibt es keine Änderung im Ergebnis im Vergleich mit § 4 DSG 2000. Der "für die Verarbeitung Verantwortlicher" bei einem Smart Car kann daher der Fahrzeughersteller, der Dienstleister aber auch der Fahrer selbst sein.

d) Auftragsverarbeiter

Ein Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet. Hier hat sich im Vergleich zur DSRL keine Neuerung ergeben. Die Bestimmungen sind fast wortgleich.

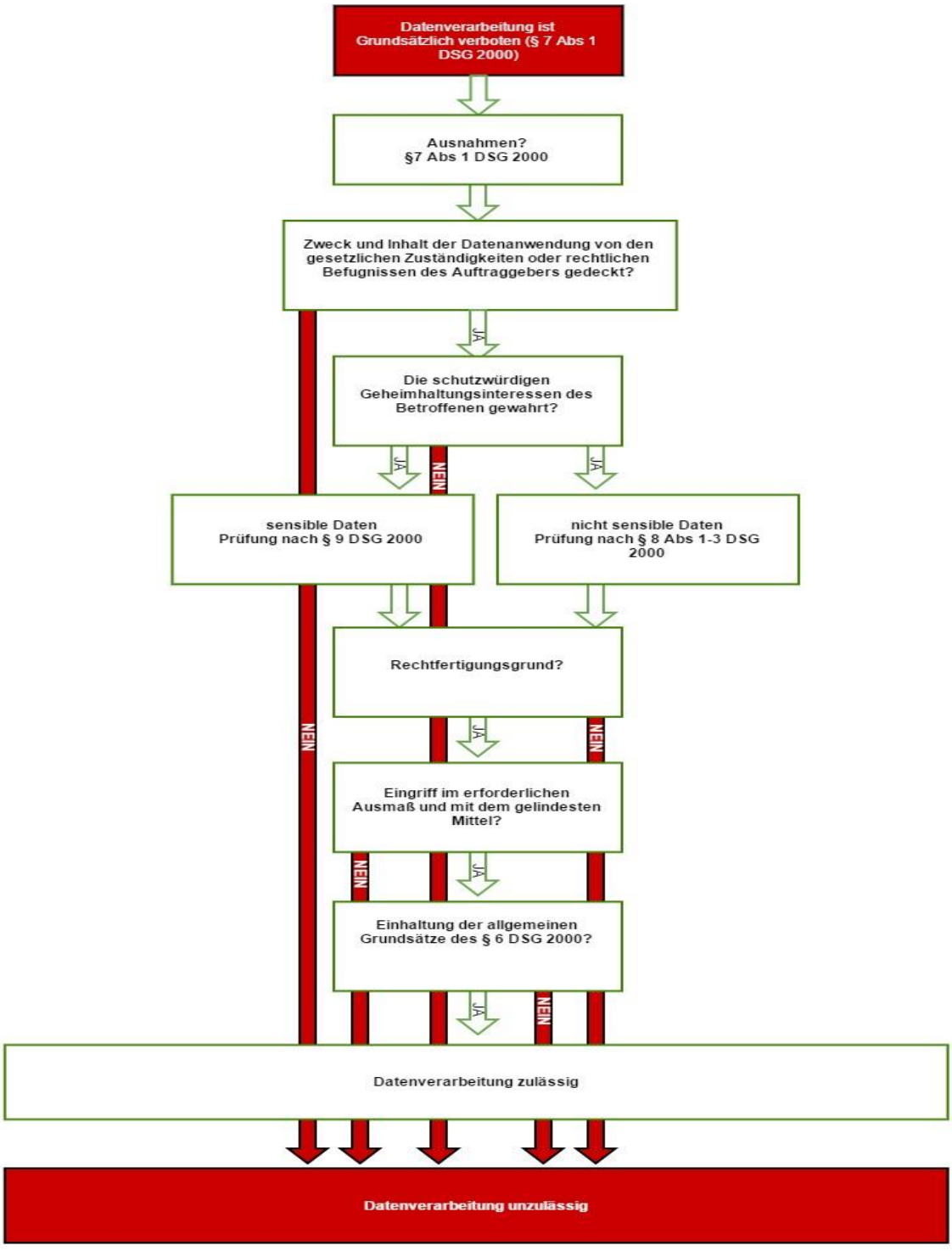
Hier kann auf die Ausführungen zum Dienstleister in III. B. d), über die Relevanz bei einem Smart Car verwiesen werden.

e) Betroffener

Ein Betroffener ist, sowohl nach der RL 95/46/EG, als auch nach der DS-GVO, eine natürliche Person, deren Daten von einem Auftraggeber verarbeitet werden (Art 4 DS-GVO). Im Falle von Smart Cars, kann bei dem Begriff „Betroffener“ auf die Ausführungen in III. B. e) verwiesen werden.

E. Datenschutzrechtliche Zulässigkeitsprüfung

Prüfungsschema der Zulässigkeitsprüfung:



1. Zulässigkeitsprüfung für das Verarbeiten der Mobilitätsdaten im Fahrzeug

Aus dem einleitenden Satz des § 7 Abs 1 DGS 2000 „Daten dürfen nur verarbeitet werden, soweit …." kann abgeleitet werden, dass grundsätzlich ein Verbot jeder Datenverarbeitung besteht (Verbotsprinzip[66]). Die Zulässigkeitsprüfung muss daher grundsätzlich mit der Feststellung beginnen, dass die Datenverarbeitung grundsätzlich verboten ist, soweit es nicht eine Ausnahme gibt[67]. Die Zulässigkeitsprüfung erfolgt mehrstufig. Die Reihenfolge folgt der Systematik des § 7 DSG 2000[68].

Folgende Voraussetzungen sind notwendig:

- Berechtigung des Auftraggebers bei der Verarbeitung von Daten
- Berücksichtigung der schutzwürdigen Interessen der Betroffenen
- Eingriff im erforderlichen Ausmaß und mit dem gelindesten Mittel
- Einhaltung der allgemeinen Grundsätze des § 6 DSG 2000

Liegen diese Voraussetzungen vor, ist die Datenverarbeitung zulässig.

a) Berechtigung des Auftraggebers gemäß § 7 Abs 1 DSG 2000

Als erster Prüfungsschritt ist die Berechtigung des Auftraggebers zu prüfen. Hierbei ist zu fragen, ob Zweck und Inhalt der Datenverwendung, im öffentlichen Bereich von der gesetzlichen Zuständigkeit des Auftraggebers, oder im privaten Bereich, von seinen sonstigen rechtlichen Befugnissen, gedeckt sind. Um diese Prüfung vornehmen zu können, muss zuerst der Zweck und Inhalt feststehen[69]. Was aber die Begriffe „Zweck" und „Inhalt" der Datenverarbeitung bedeuten, ist im DSG 2000 nicht definiert. Aus dem § 6 Abs 1 Z 2 DSG 2000 ergibt sich jedoch, dass für jede Datenverarbeitung ein bestimmter, vordefinierter Zweck festgelegt werden muss (Zweckbindungsgrundsatz). Jede spätere Änderung oder Erweiterung des Zwecks ist dann auf die Zulässigkeit zu prüfen[70].

Nach dem Wesentlichkeitsgrundsatz, muss sich die Datenverarbeitung auf die, für den angestrebten Zweck, wesentliche Datenverarbeitung beschränken. Dieser Grundsatz dient dazu den Datenumfang zu begrenzen (Datensparsamkeit). Eine Ermittlung von Daten auf Vorrat, also ohne bestimmten Verwendungszweck, ist mit § 6 Abs 1 Z 2 DSG 2000 unvereinbar[71].

---

[66] *Dohr/Pollirer/Weiss/Knyrim*, DSG 2000. Datenschutz[2] Anm 2 zu § 6 94.

[67] *Knyrim*, Datenschutzrecht[3], 105.

[68] *Jahnel*, Datenschutzrecht, Rz 4/6.

[69] *Jahnel*, Datenschutzrecht, Rz 4/8.

[70] *Jahnel*, Datenschutzrecht, Rz 4/9.

[71] Vgl VfSlg 16.369/2001.

Nach dem Grundsatz von Treu und Glauben und Rechtmäßigkeit, dürfen die Daten nur auf rechtmäßige Weise (Einhaltung sämtlicher Datenschutzbestimmungen) verwendet werden und nach dem Grundsatz der sachlichen Richtigkeit und Aktualität muss die Datenverarbeitung richtig sein[72].

Mit dem „Inhalt" meint der Gesetzgeber die, in der Datenverarbeitung (Ermitteln, Verarbeiten, Erfassen) verwendeten, Datenarten und die betroffenen Personengruppen. Neben den Datenarten muss auch klar sein, auf welche Art die Daten verarbeitet werden[73].

Denkbar wären aus meiner Sicht die Datenverarbeitungszwecke „Sicherheit der Insassen des Fahrzeuges", „Sicherung des Betriebs des Fahrzeuges durch Evaluierung der Abnützungen von Verschleißteilen", „Fehlerbehebung/Verbesserung des Services", „Pannenhilfe".

Für die oben genannten Zwecke können vom Fahrzeughersteller eine Vielzahl an Mobilitätsdaten erhoben werden. Beispiele dafür wären: zurückgelegte Strecke, Fahrtdauer, auf welcher Straße man sich befindet (Autobahn, Ortsgebiet), Geschwindigkeit, Außentemperatur, Wetter (Regen, Glatteis, Sturm), Zeitpunkt der Fahrt (Tag, Nacht), Beschleunigung, allgemeiner Zustand des Kfz (wann zuletzt ein Service gemacht wurde, Zustand der Bremsbeläge, Reifendruck) und viele weitere Daten. Gemäß dem Zweckbindungsgrundsatz, dürfen Daten nur verwendet werden, soweit sie für den Zweck wesentlich sind und nicht über den Zweck hinausgehen. Die Daten müssen damit für die Datenverwendung von wesentlicher Bedeutung sein[74]. Durch den Zweckbindungsgrundsatz müssen die Fahrzeughersteller genau untersuchen, ob die von ihnen erhobenen Daten auch wirklich benötigt werden, um die festgelegten Zwecke zu erfüllen. Dem Fahrzeughersteller ist es daher nicht erlaubt Daten zu erheben, die nicht der Evaluierung von Verschleißteilen, der Sicherheit der Insassen oder der Fehlerbehebung dienen. Es ist dem Fahrzeughersteller auch untersagt, für spätere Zwecke, einen Datenvorrat (z.B. für Data mining) aus Fahrzeugdaten anzulegen.

Daten dürfen gemäß § 6 Abs 1 Z 4 DSG 2000 nur so verwendet werden, dass sie, bezogen auf den Verwendungszweck, im Ergebnis sachlich richtig und wenn nötig, auf den neuesten Stand gebracht sind. Das bedeutet, dass die Mobilitätsdaten inhaltlich richtig erhoben und gespeichert werden müssen. Der Grundsatz der Aktualität besagt, dass Daten stets aktuell zu halten sind, damit sie auch richtig bleiben, jedoch nur soweit dies nötig ist[75].

---

[72] *Knyrim*, Datenschutzrecht[3], 95, 99; *Jahnel*, Datenschutzrecht, Rz 4/10.

[73] *Jahnel*, Datenschutzrecht, Rz 4/10; *Knyrim*, Datenschutzrecht[3], 106.

[74] *Jahnel*, Datenschutzrecht, Rz 4/106.

[75] *Knyrim*, Datenschutzrecht[3], 100.

Der Fahrzeughersteller hat zu fragen, ob es notwendig ist, die Daten zu aktualisieren und wenn ja, ob dies bereits erfolgte. Beispielsweise kann hier das Einspielen von notwendigen Fahrzeugupdates oder aktuellen Navigationskarten genannt werden.

Daten dürfen nur nach Treu und Glauben[76] und auf rechtmäßige Weise verwendet werden. Unter „auf rechtmäßige Weise" ist die Befolgung sämtlicher Datenschutzbestimmungen im DSG selbst, wie auch in allen Nebengesetzen zu verstehen[77]. Der Begriff „Treu und Glauben", welcher aus der Datenschutzrichtlinie stammt, ist nicht definiert. Es handelt sich wohl um einen sittlichen Grundsatz, ähnlich dem Grundsatz der Übung des „redlichen Verkehrs"[78]. Aus den Erläuterungen zur Regierungsvorlage ist herauszulesen, dass eine Datenverwendung dann vorliegt, wenn der Betroffene über die Umstände des Datengebrauchs und das Bestehen bzw. die Durchsetzbarkeit seiner Rechte nicht irregeführt wird[79].

Als Zwischenergebnis kann festgehalten werden, dass Zweck und Inhalt der Datenanwendungen feststehen.

Des Weiteren ist zu prüfen, ob Zweck und Inhalt der Datenanwendungen von den rechtlichen Befugnissen des Auftraggebers gedeckt sind. Diese Befugnisse können sich durch eine Konzession, Materiengesetz, Gewerbeberechtigung eines Unternehmens, den Statuten eines Vereins oder auch dem Gesellschaftsvertrag eines Unternehmens ergeben[80]. Fahrzeughersteller die eine Gewerbeberechtigung für „Karosseriebau- und Karosserielackiertechniker; Kraftfahrzeugtechnik", „Fahrzeughandel" haben können grundsätzlich jene Datenverarbeitungen vornehmen, die zur Erfüllung dieses Geschäftszwecks notwendig sind. Der Geschäftszweck umfasst die Herstellung, Reparatur, Wartung und Herstellung des sicheren Gebrauchs des Fahrzeuges. Im Ergebnis kann daher festgehalten werden, dass die genannten Zwecke „Sicherheit der Insassen des Fahrzeuges", „Sicherung des Betriebs des Fahrzeuges durch Evaluierung der Abnützungen von Verschleißteilen", „Fehlerbehebung/Verbesserung des Services" und „Pannenhilfe", durch die Gewerbeberechtigung abgedeckt sind.

b) Schutzwürdige Geheimhaltungsinteressen

Da eine rechtliche Befugnis des Fahrzeugherstellers vorliegt, ist nun in einem weiteren Schritt zu prüfen, ob durch die Datenanwendung schutzwürdige Geheimhaltungsinteressen der Betroffenen verletzt werden. Unter den schutzwürdigen Geheimhaltungsinteressen sind, ganz

---

[76] *Dohr/Pollirer/Weiss/Knyrim*, DSG 2000. Datenschutz[2] Anm 3 zu § 6 95.

[77] *Knyrim*, Datenschutzrecht[3], 95.

[78] *Knyrim*, Datenschutzrecht[3], 96.

[79] ErläutRV 1613 BlgNR 20. GP 39.; *Jahnel*, Datenschutzrecht, Rz 4/99.

[80] *Jahnel*, Datenschutzrecht, Rz 4/17.

allgemein, die Interessen des Betroffenen an der Geheimhaltung, der über ihn verarbeiteten Daten zu verstehen[81].Würden die Geheimhaltungsinteressen des Betroffenen durch die Datenanwendung verletzt werden, ist die Zulässigkeitsprüfung abzubrechen[82]. Die Datenverwendung wäre in diesem Fall verboten. Wenn die schutzwürdigen Geheimhaltungsinteressen bei einer Datenverwendung geprüft werden, die weder sensible noch strafrechtlich relevante Daten enthält, ist es sinnvoll mit der Prüfung nach § 8 Abs 2 DSG 2000 zu beginnen[83]. Schutzwürdige Interessen gelten jedenfalls dann als nicht verletzt, wenn zulässigerweise veröffentlichte Daten oder indirekt personenbezogene Daten verwendet werden. Sowohl die Fahrzeugdaten, als auch die Telematikdaten, sind weder zulässigerweise veröffentlichte, noch indirekt personenbezogene Daten.

Als nächster Prüfungsschritt ist zwischen nicht-sensiblen und sensiblen Daten zu unterscheiden. Sensible Daten dürfen nur aus den im § 9 Abs 1 DSG 2000 taxtiv aufgezählten Ausnahmen verarbeitet werden. Wie schon im Punkt III. B. b) ausführlich dargebracht, sind Mobilitätsdaten keine sensiblen Daten. Die Prüfung ist daher nach § 8 Abs 1 DSG 2000 fortzusetzen. Danach sind die schutzwürdigen Geheimhaltungsinteressen, bei nicht-sensiblen Daten, nicht verletzt wenn:

- eine ausdrückliche, gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht oder (Z 1)
- der Betroffene der Verwendung seiner Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder (Z 2)
- lebenswichtige Interessen des Betroffenen die Verwendung erfordern oder (Z 3)
- überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern (Z 4).

Ausdrückliche gesetzliche Ermächtigung oder Verpflichtung

Da es sich bei Mobilitätsdaten um nicht-sensible Daten handelt, ist nach dieser Prüfung vorzugehen. Ziffer 1 ist bei Smart Cars nicht anwendbar, da es keine Ermächtigung oder ein Gesetz gibt, welches eine ausdrückliche Verwendung der Daten vorsieht. In Betracht kommen daher nur Z 2, Z 3 und Z 4, welche nachfolgend geprüft werden.

---

[81] *Jahnel*, Datenschutz, Rz 4/19.

[82] *Unger*, Grundzüge des Datenschutzrechts[2], 21.

[83] *Jahnel*, Datenschutz, Rz 4/21.

Zustimmung

Hat der Betroffene der Verwendung seiner Daten zugestimmt, dann sind seine schutzwürdigen Geheimhaltungsinteressen gemäß § 8 Abs 1 Z 2 DSG 2000 nicht verletzt. Die Zustimmung muss nach den Kriterien des § 4 Z 14 DSG 2000 erfolgen. Ein Widerruf der Zustimmung ist jederzeit möglich und wirkt pro futuro. § 4 Z 14 DSG 2000 definiert diese Zustimmung als die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten eingewilligt hat. Gültig bedeutet, dass die Zustimmungserklärung[84] nicht ungültig oder widerrufen sein darf[85]. Schriftlichkeit ist keine Voraussetzung der Gültigkeit, ist aber für Beweiszwecke anzuraten (keine Handschriftlichkeit erforderlich, E-Mail ausreichend). Ohne Zwang bedeutet, dass die Zustimmung nicht unter physischem oder psychischem Zwang abgegeben werden darf[86]. Es darf auch nicht mit negativen Folgen gedroht werden[87]. Des Weiteren muss die Zustimmung eine Willenserklärung des Betroffenen sein. Es muss ihm klar sein, dass er eine Zustimmungserklärung abgibt. Schweigen ist, außer bei vorheriger ausdrücklicher Vereinbarung, keine Zustimmung[88]. In Kenntnis der Sachlage bedeutet, dass die Zustimmung sich auf einen bestimmten Zweck beziehen muss. Werden die Daten für einen anderen, als den ursprünglich vereinbarten Zweck verwendet, ist eine neuerliche Zustimmung einzuholen[89].

Ein großer Teil der Neufahrzeuge fallen mittlerweile in die Kategorie Smart Car. Die Frage die sich hier stellen könnte ist, ob hier von einem ökonomischen Zwang[90] gesprochen werden kann. Bei dem Kauf eines Neufahrzeuges hat der Käufer kaum mehr die Wahl, ein Fahrzeug ohne smarte Anwendungen/Funktionen zu kaufen. Die Datenspeicherung komplett zu deaktivieren, ist in den meisten Fahrzeugen nicht vorgesehen. Solange es aber noch immer auch Neufahrzeuge ohne Smart Car Funktionen gibt, kann mE nicht von einem unzulässigen Zwang gesprochen werden.

---

[84] Musterklausel für eine Zustimmungserklärung siehe *Jahnel*, Datenschutzrecht in der Praxis, 32.; *Knyrim*, Datenschutzrecht[3], 194.

[85] *Jahnel*, Datenschutz, Rz 3/131; *Knyrim*, Datenschutzrecht[3], 172.

[86] *Jahnel*, Datenschutz, Rz 3/132.

[87] *Art-29-Datenschutzgruppe*, Stellungnahme 15/2011 der zur Definition von Einwilligung, WP 187, 34. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf>.

[88] *Jahnel*, Datenschutz, Rz 3/133; *Knyrim*, Datenschutzrecht[3], 172.

[89] *Knyrim*, Datenschutzrecht[3], 172.

[90] In einer Stellungnahme hält der Allgemeiner Deutscher Automobil-Club (ADAC) fest, dass die Einwilligung des Versicherungsnehmers nicht unter ökonomischen Druck erzwungen werden darf (wie etwa durch erhöhte Prämien) <https://www.adac.de/_mmm/pdf/fi_06_payasyoudrive_versicherungstarif_1209_58324.pdf>.

Man kann daher davon ausgehen, dass die von der Judikatur und vom Gesetz im Sinn des § 4 Z 14 DSG 2000 vorgegebenen Anforderungen, an eine wirksame Zustimmung im Bereich der Smart Cars erfüllt werden können.

Ein Widerruf der Zustimmung muss jederzeit möglich sein. Diese Möglichkeit ist in § 8 Abs 1 Z 2 DSG 2000 normiert[91]. In der Judikatur wird auch verlangt, dass die Zustimmungserklärung des Betroffenen auch einen ausdrücklichen Hinweis auf die Möglichkeit des jederzeitigen Widerrufs zu beinhalten hat[92]. Mit dem Widerruf ist eine weitere Verarbeitung pro futuro unzulässig. Eine Weiterverwendung der Daten ist dann nur mehr zulässig, wenn sie sich auf einen anderen Erlaubnistatbestand des § 8 DSG 2000 stützen kann[93]. In einem Smart Car wäre die Möglichkeit eines Widerrufs leicht zu realisieren, indem es im Boardcomputer eine Möglichkeit geben würde, bei jeder Datenverwendung die Zustimmung zu geben, aber auch zu widerrufen. Bei den meisten Fahrzeugherstellern sind die Services wie eCall, Echtzeit-Verkehrsinformationen, Remote Services (in einer Smartphone-App hat man Zugriff auf Fahrzeugdaten) in einem eigenen Vertrag gebündelt. Sollte man jetzt die Zustimmung zur Datenverwendung aller Services widerrufen, funktionieren zwar diese Funktionalitäten nicht mehr, das Fahrzeug an sich funktioniert aber weiter.

Lebenswichtige Interessen des Betroffenen

Die schutzwürdigen Geheimhaltungsinteressen werden gem. § 8 Abs 1 Z 3 DSG 2000 auch dann nicht verletzt, wenn lebenswichtige Interessen des Betroffenen die Datenverwendung erfordern. Dieser Zulässigkeitsgrund macht die Datenverarbeitung in Notfallsituationen auch ohne die Zustimmung des Betroffenen zulässig[94]. Ist der Betroffene nicht in der Lage seine eigenen Interessen wahrzunehmen, ist eine Datenverwendung für lebenswichtige Interessen nur dann zulässig, wenn anzunehmen ist, dass der Betroffene in die Verarbeitung einwilligen würde, wenn er zu einer Entscheidung imstande wäre („mutmaßliche Einwilligung“)[95]. So wäre es mE möglich, dass Smart Cars, auch wenn diese Funktion durch den Fahrer deaktiviert (Zustimmung widerrufen) wurde, einen Notruf bei einem schweren Unfall absetzt, da bei einem solchen Unfall anzunehmen ist, dass der Betroffene selbst dazu nicht mehr in der Lage ist.

---

[91] *Ennöckl*, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung, in Raschauer (Hrsg) Forschung aus Staat un Recht 174, 370.

[92] *Jahnel*, Datenschutz, Rz 3/137; OGH 19.11.2002, 4 Ob 179/02f = SZ 2002/153.; OGH 20.03.2007, 4 Ob 221/06p = ecolex 2007/252, 601 (Wilhelm) = ÖBA 2007/1450, 981 (Rummel).

[93] *Ennöckl*, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung, in Raschauer (Hrsg) Forschung aus Staat un Recht 174, 370.

[94] *Jahnel*, Datenschutz, Rz 4/35.

[95] *Dammann/Simitis*, EG-Datenschutzrichtlinie, Anm 9 zu Artikel 7, 151.

Überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten

Der vierte Zulässigkeitsgrund muss in der Praxis, vor allem im privaten Bereich, für die Rechtfertigung der rechtmäßigen Verarbeitung herhalten, wenn eine Zustimmung des Betroffenen nicht eingeholt wurde[96]. Im § 8 Abs 3 DSG 2000 werden demonstrativ Fälle aufgezählt, in denen der Gesetzgeber davon ausgeht, dass die Interessen des Auftraggebers und/oder eines Dritten überwiegen. Für Smart Cars kommen die Ziffer 3 (lebenswichtiger Interessen eines Dritten), die Ziffer 4 (Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenen) und die Ziffer 5 (Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden) in Frage.

Die Datenverwendung ist zulässig, wenn sie zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich ist. Bei einer C2C Kommunikation kann z.B. ein Fahrzeug, dass an einem Unfallort vorbei fährt, diesen erkennen und sogleich einen Notruf absetzen. Möglich wäre auch, dass das verunfallte Fahrzeug selbst mit dem vorbeifahrenden Fahrzeug per Mesh-Netzwerk[97] kommuniziert und Daten über die Anzahl der Insassen, Standort und andere relevante Daten übergibt, sodass dieses automatisch Hilfe anfordern kann[98]. In diesem Szenario ist die Datenverwendung mE jedenfalls zulässig.

Die Datenverwendung ist ebenfalls zulässig, wenn sie zur Erfüllung einer vertraglichen Verpflichtung zw Auftraggeber und Betroffenen erforderlich ist. Dieser Zulässigkeitsgrund kommt in der Praxis sehr häufig vor[99], ist aber mE nicht auf die Datenverwendung in Smart Cars anzuwenden. Die Verwendung von Mobilitätsdaten durch den Fahrzeughersteller, ist für den Kaufvertrag an sich oder für die Erbringung von Reparaturen nicht notwendig[100]. Diese Daten sind vllt. für den Hersteller interessant und nützlich aber nicht erforderlich zur Erfüllung einer vertraglichen Verpflichtung. Aufgrund der Fahrzeugdaten aus denen ersichtlich ist, dass z.B. die durchschnittliche Lebensdauer eines Scheinwerfers oder der Bremsklötze überschritten wurde, könnten Verschleißteile bestellt werden, obwohl das Fahrzeug noch gar nicht in der Werkstatt zur Begutachtung war. Diese Daten wären für den Hersteller dahingehend nützlich, da diese für eine Ressourcenoptimierung der Wertschöpfungs- und Lieferkette genutzt werden könnten. Eine bloße Nützlichkeit für die

---

[96] *Jahnel*, Datenschutz, Rz 4/40.

[97] Ein Mesh-Netzwerk ist ein Funknetz, bei dem die Zugangspunkte und Basisstationen funktechnisch miteinander verbunden sind. *IT-Wissen*, Das große Online-Lexikon für Informationstechnologie <http://www.itwissen.info/definition/lexikon/Mesh-Netz-WMN-wireless-mesh-network.html >.

[98] *Hansen*, Das Netz im Auto & das Auto im Netz, DuD 2015, 370.

[99] *Jahnel*, Datenschutz, Rz 4/47.

[100] *Weisser/Färber*, Rechtliche Rahmenbedingungen bei Connected Car Überblick über die Rechtsprobleme der automobilen Zukunft, MMR 2015, 509.

Vertragserfüllung reicht jedoch nicht aus[101]. Anders wäre dies zu beurteilen, wenn mit dem Hersteller auch ein Wartungsvertrag abgeschlossen wurde.

Wurden die Daten rechtmäßig ermittelt und ist die Datenverwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig, ist diese ebenfalls zulässig. Dadurch soll der Auftraggeber die Möglichkeit haben, seine Rechtsansprüche zu verteidigen oder auch durchzusetzen. Behauptet z.B. der Fahrer eines Smart Cars, dass die Bremsen automatisch ausgelöst wurden[102] und deshalb ein Unfall entstanden ist, soll der Fahrzeughersteller die Möglichkeit haben, den Datenspeicher auszulesen, um die Behauptungen zu widerlegen.

Zusammengefasst kann daher festgehalten werden, dass die schutzwürdigen Geheimhaltungsinteressen des Betroffenen iSd § 8 Abs 1 DSG 2000 gewahrt werden.

c) Erforderliches Ausmaß und gelindestes Mittel

Gemäß § 7 Abs 3 DSG 2000 dürfen Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen, damit die Datenverwendung zulässig ist. Des Weiteren sind die Grundsätze des § 6 DSG 2000 einzuhalten. Das Gebot des gelindesten Mittels ist die einfachgesetzliche Ausformulierung des verfassungsrechtlichen Grundrechts auf Datenschutz in § 1 Abs 2 letzter Satz DSG 2000[103].

Das gelindeste Mittel ist das schonendste, zur Verfügung stehende Mittel. Grundsätzlich ist zuerst der Betroffene zu fragen, ob er der Verwendung seiner Daten zustimmt[104]. Hier stellt sich die Frage, ob statt einer Opt-Out Option, eine Opt-In Möglichkeit zur Datenverwendung als gelinderes Mittel implementiert werden sollte. Dem könnte man entgegenhalten, dass der Zweck der Sicherheit uU nicht mehr erfüllt werden kann, da zu wenige Daten für eine Auswertung vorhanden sind. Aufgrund der DS-GVO ist durch das Prinzip von Privacy by default eine Opt-In Option nicht mehr möglich. Privacy by design bedeutet nämlich, dass die Voreinstellung in einem technischen System immer die datenschutzfreundlichste Einstellung sein muss.

---

[101] *Jahnel*, Datenschutz, Rz 4/47.

[102] *Futerzone*, Forscher hacken Corvette mittels SMS <http://futurezone.at/digital-life/forscher-hacken-corvette-mittels-sms/146.458.778>.

[103] *Jahnel*, Datenschutz, Rz 4/96.

[104] *Unger*, Grundzüge des Datenschutzrechts[2], 36.

d) Allgemeine Grundsätze des § 6 DSG 2000

Die allgemeinen Grundsätze sind in § 6 Abs 1 DSG 2000 geregelt. Sie gelten für jede Datenanwendung, als auch für jede Datenübermittlung:

- Treu und Glauben (Fairness) und Rechtmäßigkeit (Abs 1 Z 1),
- strikte Zweckbindung (Abs 1 Z 2),
- Wesentlichkeit/Begrenzung des Datenumfangs (Datensparsamkeit) (Abs 1 Z 3),
- sachliche Richtigkeit und Aktualität (Abs 1 Z 4),
- zeitliche Begrenzung (Datenlöschung).

Die Grundsätze von Treu und Glauben und Rechtmäßigkeit, Zweckbindung, Wesentlichkeit sowie sachlichen Richtigkeit und Aktualität wurden bereits bei der Prüfung der Berechtigung des Auftraggebers in lit a) ausführlich erläutert und daher kann auf diese Ausführungen verwiesen werden.

Zu beachten ist der Grundsatz der Datenlöschung gemäß § 6 Abs 1 Z 5 DSG 2000. Gemäß § 6 Abs 1 Z 5 DSG dürfen Daten nur solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist. Bei den ermittelten Daten eines Smart Cars bedeutet das, dass die ermittelten Daten, wenn sie für die oben genannten Zwecke (Sicherheit der Insassen des Fahrzeuges, Pannenhilfe, …) nicht mehr notwendig sind, entweder gelöscht oder nur in anonymisierter Form[105] aufbewahrt werden dürfen[106]. Bestimmte Daten, welche die Sicherheit im Fahrzeug während der Fahrt betreffen (Positionsdaten, Geschwindigkeit, Anzahl der Insassen) und nur für einen Unfall relevant sind, sind also nach jedem Fahrtende zu löschen oder zumindest zu anonymisieren. Andere Daten wie z.B. der Abnutzungsgrad von Verschleißteilen, sind nach jedem Werkstattbesuch/Reparatur der betreffenden Teile zu löschen oder zu anonymisieren. Die erhobenen Daten sind mE nach diesem Zeitpunkt als unzulässig verarbeitete Daten zu beurteilen und sind zu löschen.

Im Ergebnis kann die Datenerfassung und –speicherung in einem Smart Car datenschutzrechtlich zulässig sein. Die Frage ist, ob die Zwecke der Datenverwendung genau genug definiert sind und ob die schutzwürdigen Geheimhaltungsinteressen des Betroffenen gewahrt werden. In der Praxis wird meist eine gültige Zustimmungserklärung des Betroffenen

---

[105] A*rt-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, 0829/14/DE, <ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf>.

[106] *Jahnel*, Datenschutz, Rz 4/110.

vorliegen. Für die in III. E. 1. a) beschriebenen Zwecke, ist mE eine Datenerfassung und –speicherung datenschutzrechtlich zulässig.

2. Zulässigkeit der Übermittlung

Gemäß § 4 Z 12 DSG 2000 ist das Übermitteln von Daten, die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen von Daten. Eine Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers ist ebenfalls eine Übermittlung von Daten iSd § 4 Z 12 DSG 2000.

Die Datenermittlung kann daher nur in drei verschiedenen Formen auftreten[107]:

1. Weitergabe an einen Dritter, der nicht Betroffener, Auftraggeber oder Dienstleister ist
2. Veröffentlichung von Daten
3. Wenn die Daten für ein anderes Aufgabengebiet des Auftraggebers genutzt werden

Auf den Fall der Smart Cars umgelegt, ist die Datenübertragung zwischen dem Fahrzeug und den Servern des Fahrzeugherstellers kein Übermitteln iSd § 4 Z 12 DSG 2000, da in diesem Verhältnis der Fahrzeughersteller Auftraggeber ist. Wenn also der Auftraggeber die Daten an sich selbst überträgt/sendet, liegt keine datenschutzrechtliche Übermittlung vor. Die Weitergabe der Daten zwischen Auftraggeber und Dienstleister, im Rahmen des Auftragsverhältnisses, wird als Überlassen in § 4 Z 11 DSG 2000 definiert. Daraus folgt, dass sowohl bei der Übertragung der Daten zwischen Fahrzeug und Fahrzeughersteller, als auch zwischen Fahrzeug und Dienstleister, die Bestimmungen des §§ 7 ff DSG 2000 nicht anzuwenden sind, da keine datenschutzrechtliche Übermittlung stattfindet.
Eine Übermittlung wäre nur dann zu prüfen, wenn die Mobilitätsdaten veröffentlicht wurden, der Fahrzeughersteller die Daten für einen anderen Zweck verwendet oder der Fahrer selbst zum datenschutzrechtlichen Auftraggeber wird. Beispiele dafür wären die Synchronisierung der Kontakte zwischen Mobiltelefon und Fahrzeug oder auch das Speichern von personalisierten Einstellungen im Fahrzeug.

3. Überlassen der Daten an einen Dienstleister

Wie schon in den technischen Grundlagen beschrieben, werden von Smart Cars eine große Anzahl an Daten gesammelt. Alleine aufgrund der Kosten und des benötigten Know-Hows, scheint es sinnvoll sich eines Dienstleisters zu bedienen, welcher für die Verarbeitung der

[107] *Jahnel*, Datenschutz, Rz 3/116.

Mobilitätsdaten verantwortlich ist. Dienstleister im Sinn des § 4 Z 5 DSG 2000 ist eine natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft, beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden (verarbeiten und übermitteln). Die Daten, welche der Dienstleister von dem Fahrzeughersteller (Auftraggeber) erhalten hat, dürfen nur zu dem vom Fahrzeughersteller vorgegebenen Zweck verwendet werden. Werden die Daten zu eigenen Zwecken des Dienstleisters verarbeitet, wird der Dienstleister selbst zum datenschutzrechtlichen Auftraggeber.

Die grundsätzliche Voraussetzung für die Zulässigkeit der Überlassung ist, dass die Daten zulässigerweise verarbeitet wurden[108]. Aus der Zulässigkeitsprüfung (siehe E. 1.) hat sich für unseren Fall ergeben, dass die Datenverwendung zulässig war. Würden wir hier zu dem Ergebnis kommen, dass die Datenverwendung beim Auftraggeber selbst schon unzulässig war, scheidet eine Zulässigkeit der Datenüberlassung an einen Dienstleister aus[109].

Gemäß § 10 Abs 1 DSG 2000 darf ein Auftraggeber (Fahrzeughersteller) bei seinen Datenanwendungen Dienstleister in Anspruch nehmen, wenn diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten. Der Auftraggeber hat mit dem Dienstleister, die hierfür notwendigen Vereinbarungen zu treffen und sich von ihrer Einhaltung durch Einholung der erforderlichen Informationen über die vom Dienstleister tatsächlich getroffenen Maßnahmen zu überzeugen. Der Formulierung der § 10 Abs 1 1. Satz DSG 2000 ist eine Prüfpflicht des Auftraggebers zu entnehmen. Diese Prüfpflicht beinhaltet, dass sich der Auftraggeber zumindest eine entsprechende Gewerbeberechtigung vorlegen lässt[110]. Je sensibler die betreffenden Daten, desto sorgfältiger wird ein Auftraggeber zu überprüfen haben, wie weit ein zukünftiger Dienstleister als geeignet im Sinne des § 10 DSG 2000 angesehen werden kann, bzw. welche Verpflichtungen einem solchen Dienstleister, aus datenschutzrechtlicher Sicht, vertraglich auferlegt werden müssen[111].Die Pflichten des Dienstleisters sind in § 11 DSG 2000 normiert, bestehen bereits kraft Gesetzes und bedürfen daher keiner weiteren vertraglichen Vereinbarung[112]. Gemäß § 11 Abs 2 DSG 2000 muss erst die nähere Ausgestaltung dieser Pflichten, zum Zweck der Beweissicherung, schriftlich festgehalten werden.

---

[108] *Jahnel*, Datenschutz, Rz 3/55.

[109] *Jahnel*, Datenschutz, Rz 3/55.

[110] *Jahnel*, Datenschutz, Rz 3/56.

[111] Datenschutzkommission K211.413/006-DSK/2002.

[112] *Dohr/Pollirer/Weiss/Knyrim*, DSG 2000. Datenschutz[2], § 11 Anm 3, 146.

Der Dienstleister hat gemäß § 11 DSG 2000 die Pflicht

- die Daten ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden (Z 1)
- alle gemäß § 14 DSG 2000 erforderlichen Datensicherheitsmaßnahmen zu treffen (Z 2)
- weitere Dienstleister nur mit Zustimmung des Auftraggebers heranzuziehen und deshalb den Auftraggeber von der beabsichtigten Heranziehung eines weiteren Dienstleisters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann (Z 3)
- im Einvernehmen mit dem Auftraggeber die notwendigen technischen und organisatorischen Voraussetzungen für die Erfüllung der Auskunfts-, Richtigstellungs- und Löschungspflicht des Auftraggebers zu schaffen (Z 4)
- nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten (Z 5)
- und dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der genannten Verpflichtungen notwendig sind (Z 6)[113].

Sind die Voraussetzungen des § 10 DSG 2000 und des § 11 DSG 2000 (Pflichten des Dienstleisters) erfüllt, kann der Fahrzeughersteller einen Dienstleister mit dem Verarbeiten der Mobilitätsdaten beauftragen[114]. Eine weitere Prüfung, ob die Mobilitätsdaten an den Dienstleister überlassen werden dürfen, ist nicht erforderlich, sofern das Überlassen der Daten an einen Dienstleister innerhalb Österreichs oder innerhalb der EU erfolgt[115]. Soll die Überlassung aber an einen Dienstleister außerhalb der EU erfolgen, so muss die Prüfung nach § 12 DSG 2000 (Genehmigungsfreie Übermittlung und Überlassung von Daten in das Ausland) und § 13 DSG 2000 (Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland) erfolgen[116]. Gemäß § 12 DSG 2000 ist das Übermitteln von Daten an Dienstleister außerhalb des EWR dann zulässig, wenn sich der Dienstleister in einem Drittstaat mit angemessenem Datenschutz[117] befindet (§ 12 Abs 2 DSG 2000) oder einer der Fälle, die in § 12 Abs 3 DSG 2000 aufgezählt sind vorliegt. Am relevantesten sind hier das Überlassen von nur indirekt personenbezogenen Daten (Z 2) oder eine Zustimmung des Betroffenen (Z 5). Laut Statistik Austria sind ca. 75 Prozent der im Jahr 2015 zugelassenen

[113] siehe ausführlich *Jahnel*, Datenschutz, Rz 3/59 – 3/67.

[114] *Knyrim*, Datenschutzrecht[3], 206.

[115] *Knyrim*, Datenschutzrecht[3], 207.

[116] *Knyrim*, Datenschutzrecht[3], 207.

[117] dazu zählen gemäß § 1 DSAV: Schweiz, Argentinien, Guernsey, Insel Man, Jersey, Färöer Inseln, Andorra, Uruguay, Neuseeland, USA (im Moment nur durch Genehmigung der DSB oder Standardvertragsklausel, im Moment wird an einem Nachfolger des „Safe-Harbor" gearbeitet mit dem Titel EU-US-Privacy-Shield), Kanada, Israel.

Fahrzeugmarken, Fahrzeuge bei denen der Hersteller seinen Sitz in Europa hat. Die Restlichen 25 Prozent verteilen sich auf die USA und Asien. Für die meisten Hersteller ist es also möglich, einen Dienstleister mit der Verarbeitung der Mobilitätsdaten an ihrem Standort zu beauftragen.

F. Datensicherheit

1. Risiken

Datensicherheit bei Smart Cars ist heute durch diverse Hackerangriffe ein wichtiges Thema. Die gesammelten Mobilitätsdaten besitzen einen hohen Wert ua für Big Data Anwendungen und daher kann auch mit einem Hackerangriff gerechnet werden. Da eine große Anzahl an Schnittstellen wie Bluetooth, WLAN, NFC vorhanden sind, können Daten von Smart Cars manipuliert werden, wenn Hacker Zugriff durch diese Schnittstellen erlangen. Dadurch können einzelne Komponenten des Fahrzeugs, aber auch das gesamte Fahrzeug, beeinträchtigt werden. Immer öfters liest man in den verschiedensten Medien über Hackerangriffe an Fahrzeugen oder welche Marke Sicherheitslücken in ihrem System hat[118]. Diese Lücken können aber auch schwere Unfälle verursachen, wenn während der Fahrt auf einer Autobahn das Fahrzeug manipuliert wird, indem die Bremsen plötzlich aktiviert werden[119] oder einfach der Motor abgeschaltet wird[120]. Großen Schaden für die Wirtschaft verursacht im Moment auch die sogenannte „Rasomware". Dabei handelt es sich um eine Schadsoftware, die Daten verschlüsselt und den Zugriff darauf verhindert. Damit die Funktionalität wieder hergestellt werden kann, indem die Daten wieder entschlüsselt werden, muss der Betroffene dem Angreifer eine Lösegeldsumme für den Schlüssel bezahlen. 5.000-mal pro Stunde verbreitet sich die neue Rasomware „Locky" alleine in Deutschland[121]. Noch ist kein Angriff auf Smart Cars bekannt, aber sobald die kritische Masse der Anzahl an Fahrzeugen erreicht ist, damit sich der Aufwand die Schadsoftware an Fahrzeuge anzupassen auszahlt, wird es sicher auch dafür eine solche Malware geben. Der Angreifer könnte aber

---

[118] *Der Standard*, „Die Gefahr ist real":Auto-Hacks schrecken Branche auf, <http://derstandard.at/2000022195679/Die-Gefahr-ist-real-Auto-Hacks-schrecken-Branche-auf>; *Frankfurter Allgemeine Zeitung*, Jetzt auch Tesla-Auto gehackt < http://www.faz.net/aktuell/wirtschaft/neue-mobilitaet/sicherheitsforscher-hacken-nach-jeep-hack-auch-tesla-auto-13738472.html>.

[119] *Futurezone*, Forscher hacken Corvette mittels SMS <http://futurezone.at/digital-life/forscher-hacken-corvette-mittels-sms/146.458.778>.

[120] *Wired*; Hackers Remotely Kill a Jeep on the Highway—With Me in It <http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>.

[121] *Heise online*, Krypto-Trojaner Locky wütet in Deutschland: Über 5000 Infektionen pro Stunde<http://www.heise.de/newsticker/meldung/Krypto-Trojaner-Locky-wuetet-in-Deutschland-Ueber-5000-Infektionen-pro-Stunde-3111774.html>.

nicht nur den einzelnen Fahrzeughalter erpressen, sondern der Angriff könnte auch dem Hersteller gelten, indem das gesamte Rechenzentrum des Herstellers bedroht wird. Diese Risiken kann man durch geeignete Sicherheitsmaßnahmen minimieren, jedoch nicht restlos eliminieren.

2. Maßnahmen

Personenbezogene Daten sind so schutzwürdig, dass trotz rechtmäßiger Verarbeitung, gesonderte Datensicherheitsmaßnahmen einzuhalten sind[122]. Die Datensicherheit ist in § 14 DSG 2000 geregelt. Danach sind alle Organisationseinheiten des Auftraggebers oder Dienstleisters (Fahrzeugherstellers) verpflichtet, Maßnahmen zum Schutz der Daten zu treffen. Welche Maßnahme zu treffen ist, hat gemäß § 14 Abs 1 letzter Satz DSG 2000 unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit zu erfolgen. Je „heikler" die verwendeten Daten, desto größer/besser müssen die Sicherheitsvorkehrungen sein[123].
Die Datensicherheit ist aber jedenfalls dann gegeben wenn sichergestellt ist, dass

- die Daten vor zufälliger oder unrechtmäßiger Zerstörung geschützt sind
- die Daten vor Verlust geschützt sind,
- ihre Verwendung ordnungsgemäß erfolgt und
- dass die Daten Unbefugten nicht zugänglich sind

§ 14 Abs 2 DSG 2000 führt des Weiteren noch Datensicherheitsmaßnahmen an, wie z.B. ausdrückliche Festlegung der Aufgabenverteilung bei der Datenverwendung, Verwendung von Daten an das Vorliegen gültiger Aufträge zu binden, Regelung von Zutrittsberechtigungen zu Räumlichkeiten, Zugriffsberechtigung auf Daten und Programme, Belehrung der Mitarbeiter, Protokollführung, Dokumentationspflicht, Aufbewahrungspflicht. Wird die Datensicherheit nicht eingehalten ist neben zivilrechtlichen Schadenersatzansprüchen, eine Verwaltungsstrafe bis zu 10.000 EUR möglich. Mit der DS-GVO ist hier eine Strafe von bis zu 10 Mio. EUR oder 2% des weltweiten Konzernumsatzes möglich.

Fahrzeughersteller haben daher sowohl das Fahrzeug selbst (Zutritt), als auch die Kommunikation (auch zu externen Geräten) und jede Art von Schnittstelle, nach dem Stand der Technik auf technischer Ebene zu verschlüsseln, um dadurch Zugriffe durch

---

[122] *Unger*, Grundzüge des Datenschutzrechts[2], 45.

[123] *Knyrim*, Datenschutzrecht[3], 372

Unberechtigte zu verhindern. Zusätzlich ist ein Protokoll über entstandene Fehler und Zugriffe zu führen. Persönliche Nutzerprofile, die Voreinstellungen in Fahrzeugen speichern, müssen durch eine individuelle Abfrage vor fremdem Zugriff geschützt werden (z.B. PIN Abfrage). Die Fahrzeuge müssen des Weiteren über eine Manipulationserkennung verfügen, welche eine Datenintegrität gewährleistet. Bei zur Verfügungstellung einer Smartphone App, um das Fahrzeug aus der Ferne zu starten, die Sitzheizung zu Bedienen oder auch nur den Tankinhalt auszulesen, hat die Verbindung über eine verschlüsselte Verbindung nach dem Stand der Technik (z.B. SSL) zu erfolgen und der Nutzer hat sich bei der Anmeldung zu authentifizieren. Die Daten müssen nach Erreichung der Zwecke, für die sie ermittelt wurden, gelöscht werden. Möchte man das Fahrzeug weiterverkaufen, sollte man die Möglichkeit haben, alle Mobilitätsdaten löschen oder anonymisieren zu können, damit eine Rückverfolgbarkeit zu dem vorigen Besitzer nicht mehr möglich ist.

G. Meldepflicht

Ist eine Datenanwendung bei einem Smart Car meldepflichtig? Eine Datenanwendung ist gemäß § 4 Z 7 DSG 2000, die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (verarbeiten und übermitteln), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung). Als Datenanwendung bei einem Smart Car würde mE nach ua „Monitoring und Wartung von Kundenfahrzeugen“ in Betracht kommen.

Aus dem Gesetz lässt sich sowohl eine Pflicht zur Meldung vor Aufnahme einer Datenanwendung ableiten, als auch die Pflicht diese Meldung immer aktuell zu halten[124]. Ausnahmen dieser Meldepflicht sind in § 17 Abs 2 DSG 2000 geregelt. Ausgenommen von der Meldepflicht ist die Verarbeitung von ausschließlich veröffentlichten Daten (Z 1), Daten für die Führung von öffentlichen Registern oder Verzeichnissen (Firmenbuch, Grundbuch) (Z 2), die nur indirekt personenbezogene Daten enthalten (anonyme Daten) (Z 3), von natürlichen Personen ausschließlich für persönliche oder familiäre Tätigkeiten vorgenommen werden (wichtigste Ausnahme für Privatpersonen da sonst jeder PC meldepflichtig wäre) (Z 4) für publizistische Tätigkeit (Z 5) oder einer Standardanwendung entsprechen (wichtigste Ausnahme für Unternehmen)[125]. Zu klären ist auch, ob eine Vorabkontrolle iSd § 18 Abs 2

[124] *Knyrim*, Datenschutzrecht[3], 50.

[125] *Knyrim*, Datenschutzrecht[3], 52.

DSG 2000 erforderlich ist. Da es sich dabei um eine taxative Aufzählung handelt, wäre diese nur dann erforderlich, wenn die Datenanwendung sensible Daten oder strafrechtlich relevante Daten im Sinne des § 8 Abs 4 DSG 2000 enthält, die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck hat, oder in Form eines Informationsverbundsystems durchgeführt werden soll. Eine Aufnahme der Datenanwendung wäre dann erst nach Genehmigung durch die DSB möglich. Wie schon im Kapitel Begriffsbestimmungen näher erörtert, sind Mobilitätsdaten jedoch keine sensiblen Daten iSd § 4 Z 2 DSG 2000.

Im Ergebnis kann daher festgehalten werden, dass die Datenanwendung „Monitoring und Wartung von Kundenfahrzeugen" jedenfalls meldepflichtig ist, da sie unter keine Ausnahme des § 17 Abs 2 DSG 2000 subsumiert werden kann. Eine Vorabkontrolle ist jedoch aufgrund der oben näher erläuterten Voraussetzungen nicht erforderlich.

IV. Ausblick DS-GVO

Der Datenschutz wird in den nächsten Jahren für Unternehmen immer wichtiger werden. Nicht unbedingt weil diese mehr Interesse daran gefunden haben, die Daten, ua ihrer Kunden zu schützen, sondern weil ab ca. Mitte 2018 die neue Datenschutzgrundverordnung in Kraft tritt, die weitgehend das nationale Datenschutzgesetz ersetzt. Die Verordnung ist unmittelbar anwendbar, trotzdem sind einige Teile auf nationaler Ebene umzusetzen (hinkende Verordnung). Die Unternehmen werden alleine schon deshalb mehr auf den Datenschutz achten, da sich der Strafrahmen für Verstöße drastisch ändern wird. War die Höchststrafe im DSG 2000 mit maximal 25.000 EUR[126] begrenzt, so sind in der DS-GVO Strafen bis zu 20 Millionen EUR oder 4% vom globalen Konzernumsatz möglich (im Fall von Google wäre eine Maximalstrafe von 3 Milliarden USD[127] möglich). Kein Wunder also, dass der Datenschutz für viele Unternehmen bisher kein wichtiges Thema war. Datenschutz wurde maximal aus Imagegründen für Werbezwecke eingesetzt, denn die Strafen die von der DSB verhängt werden konnten, stellten keinen großen Anreiz dar, die Datenschutzvorkehrungen auszubauen. Durch die Änderungen wird das Datenschutzrecht auf eine Ebene mit anderen Compliance Themen, wie Korruptionsbekämpfung und Wettbewerbsrecht gehoben. Die DS-GVO bringt aber auch sonst wichtige Neuerungen für Unternehmen, angefangen von einem zu bestellenden Datenschutzbeauftragten unter bestimmten Voraussetzungen[128], bis hin zu

[126] § 52 Abs 1 DSG 2000.

[127] *wallstreet:online* <http://www.wallstreet-online.de/aktien/alphabet-c-aktie/bilanz>.

[128] Artikel 37 ff DS-GVO.

einer Datenschutzfolgeabschätzung. Neu ist auch die Verpflichtung zu privacy by design (Datenschutz durch Technik) und privacy by default (Datenschutz als Voreinstellung). Privacy by design[129] bedeutet, dass bereits in der Entwicklungsphase neuer Technologien, die datenschutzrechtlichen Anforderungen sowie die Datensicherheit berücksichtigt und in das Produkt integriert werden müssen[130]. Der privacy by design Grundsatz umfasst ua Anonymisierungs- und Pseudonymisierungstechniken, integrierte Verschlüsselungsmethoden (SSL, AES…), Nutzer-Authentifizierungen, grundsätzliche Datensparsamkeit und die Trennung von Identifizierungs- und Inhaltsdaten[131]. Privacy by default[132] bedeutet, dass die Voreinstellung in einem technischen System immer die datenschutzfreundlichste Einstellung sein muss. Der Betroffene muss, damit personenbezogene Daten verarbeitet werden, diese Einstellungen aktiv ändern. Dadurch soll von Anfang an der Datenschutz des Betroffenen gewahrt werden. Für Fahrzeughersteller von Smart Cars bedeutet diese Neuerung, dass die Werkseinstellungen datenschutzfreundlich sein müssen und jeder Fahrer die Möglichkeit haben muss, individuelle Datenschutzeinstellungen vornehmen zu können und somit seine Einwilligung bewusst zu erklären oder zu verweigern[133]. Eine Möglichkeit wäre die Anmeldung (Authentifizierung) der einzelnen Fahrer am Fahrzeug z.B. durch den Schlüssel oder im Fahrzeug selbst (Boardcomputer) der das Datenschutzprofil speichert[134]. Die entstandenen Daten müssten zu jeder Zeit einsehbar sein und vorgenommene Einstellungen müssen einfach zurückgesetzt werden können. Änderungen durch die DS-GVO betreffen auch die Informationspflichten[135] des Auftraggebers an den Betroffenen, da diese erweitert werden. Auch das Auskunftsrecht des Betroffenen wird ua um die Auskunft der Speicherdauer und eine Rechtsmittelbelehrung ergänzt[136]. Neben den bisherigen Betroffenenrechten wird es zukünftig auch noch das Recht auf Vergessenwerden[137] und das Recht auf Datenportabilität[138] geben. Interessant für Fahrzeughersteller wird hier eher das Recht auf Datenportabilität sein. Dadurch haben die Betroffenen (Fahrzeughalter, Fahrer,…) das Recht, ihre Daten in

---

[129] Artikel 25 Abs 1 DS-GVO.

[130] *Kipker,* Privacy by Default und Privacy by Design, DuD 2015, 410.

[131] *Rost/Bock,* Privacy By Design und die Neuen Schutzziele, DuD 2011, 31. ;*Kipker,* Privacy by Default und Privacy by Design, DuD 2015, 410.

[132] Artikel 25 Abs 2 DS-GVO.

[133] *Bönninger*, Mobilität im 21. Jahrhundert: sicher, sauber, datengeschützt, DuD 2015, 389.

[134] *Bönninger/Schüppel,* Vertrauen erhalten – Datenschutz und Datensicherheit bei modernen Fahrzeugen, ZVR 2015, 478.

[135] Artikel 13 ff DS-GVO.

[136] Artikel 15 DS-GVO.

[137] Artikel 17 DS-GVO.

[138] Artikel 20 DS-GVO.

maschinenlesbarer Art zu erhalten und an ein anderes Unternehmen zu übertragen. Wenn technisch möglich, sollen die Daten direkt zwischen den Unternehmen übertragen werden. Als Umsetzung könnte ich mir bei Gebrauchtfahrzeugen vorstellen, dass man sein Datenschutzprofil von einem Fahrzeug z.B. auf einen Datenträger (evtl. USB-Stick) übertragen kann und dieses Profil in ein anderes Fahrzeug mitnehmen kann. Bei Neufahrzeugen sollten die Hersteller untereinander die Daten transferieren und das bereits bestehende Profil in das Neufahrzeug implementieren. Eine weitere Änderung betrifft die Meldepflicht des Auftraggebers vor Aufnahme einer Datenanwendung. Bisher musste die Meldung bei der DSB erfolgen, welche die Meldung im DVR registrierte. Mit der DS-GVO hat ein Unternehmen nun selbst die Pflicht, ein solches internes Register zu führen. Dies gilt nicht nur für Auftraggeber, sondern auch für Dienstleister. Auch Dienstleister müssen für jeden ihrer Auftraggeber ein eigenes Verfahrensverzeichnis führen. Der Inhalt ist weitegehend ident mit den bisherigen DVR-Meldungen, allerdings bestehen keine Ausnahmen für Standardanwendungen, da es diese nicht mehr geben wird. Zusätzlich ist die Speicherdauer anzugeben und anzuführen, ob mit der Verarbeitung ein Dienstleister beauftragt wurde. Eine weitere Neuerung ist die Pflicht zur Datenschutz Folgenabschätzung. Diese ist vom für die Verarbeitung Verantwortlichen, insbesondere bei der Verwendung neuer Technologien, durchzuführen, wenn voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten besteht. Insbesondere bei Profiling, umfangreichen Verarbeitungen sensibler oder strafrechtlich relevanter Daten, systematische Überwachung öffentlich zugänglicher Bereiche ist eine solche Folgenabschätzung durchzuführen[139]. Die DSB wird eine Liste der Verarbeitungen, bei denen eine Datenschutz-Folgenabschätzung notwendig ist, erstellen. Leider nicht geregelt wurde, wer Eigentümer der Daten, die z.B. in einem Fahrzeug entstehen, ist. Ist der Fahrzeughersteller der Eigentümer der Daten und kann damit machen was er will? Hat der Käufer des Fahrzeugs alle Rechte an den Daten? Hat vllt. der Hersteller das Recht die allg. Fahrzeugdaten zu verwenden und der Halter, die Daten, die durch den Betrieb entstehen? Um diesen unsicheren Zustand zu beseitigen, wird es für Unternehmen die praktikabelste Lösung sein, eine Klausel in die allgemeinen Geschäftsbedingungen oder den Vertrag aufzunehmen, die dem Unternehmen erlaubt, nicht personenbezogene und anonymisierte Daten für kommerzielle Zwecke zu verwenden.

Im Großen und Ganzen wird die DS-GVO einen Mehraufwand für die Hersteller von Smart Cars darstellen. Für die Betroffenen hingegen wird die Benutzung eines solchen Fahrzeuges datenschutzrechtlich sicherer.

---

[139] Artikel 35 DS-GVO.

V. Schlussbemerkung

A. Zusammenfassung

Smart Cars erzeugen und speichern eine große Anzahl an Daten. Datenschutzrechtlich ist sowohl die Datenerfassung und –speicherung in einem Smart Car für die genannten Zwecke, als auch die Überlassung der Daten an einen Dienstleister zulässig. Eine datenschutzrechtliche Übermittlung findet bei der Übertragung der Mobilitätsdaten an den Fahrzeughersteller oder an den Dienstleister nicht statt. Entscheidend für eine Zulässigkeit ist, dass die schutzwürdigen Interessen des Betroffenen gewahrt werden. Hier haben die Hersteller die Zwecke der Datenverwendung zu definieren und in den meisten Fällen eine Zustimmung des Betroffenen einzuholen. Wenn Daten für Big Data Anwendungen verwendet werden sollen, empfiehlt es sich, eine Vereinbarung über die kommerzielle Verwendung anonymisierter Daten mit dem Betroffenen zu treffen.

Als kritische Anmerkung möchte ich noch die Frage in den Raum stellen, wohin die Menge an Assistenzsystemen führen soll. Verlernt der Fahrer dann nicht das Einparken, wenn nur mehr der Parkassistent verwendet wird? Verliert man nicht die Orientierung, wenn man nur noch das Navigationssystem verwendet? Wie weit wird auch die Kontrolle gehen? Hier wird die Zukunft zeigen, in welche Richtung sich die Mobilität entwickelt. Letztendlich liegt es an der Gesellschaft zu entscheiden, wieweit diese Systeme Sicherheit oder Kontrolle bringen.

B. Abstract

Smart Cars generate and store a huge amount of data. In terms of data protection, both the data generation and –storage in a smart car, regarding the mentioned purposes, as well as the transfer of data to a processor is allowed. A transmission in terms of data protection does not occur in the transfer of mobility data to the vehicle manufacturer or the processor. It is crucial for admissibility, that the legitimate interests of the data subject are guaranteed. Manufacturers have to define the purpose of data usage and obtain an individual's consent in most cases. If data is used for Big Data applications, it is advisable to reach an agreement on the commercial use of anonymous data with the data subject.

As critical remark I would like to pose a question, where all assistance systems will lead us. Will the driver unlearn how to park a car if he only uses the parking assistant? Do you lose the orientation if you only use the navigation system? How far will the control go? The future will show how the use of mobility will develop. Finally, it is up to society to decide if these assistance systems bring security or surveillance.

VI. Literatur

Bönninger, Mobilität im 21. Jahrhundert: sicher, sauber, datengeschützt, DuD 2015, 388

Bönninger/Schüppel, Vertrauen erhalten – Datenschutz und Datensicherheit bei modernen Fahrzeugen, ZVR 2015, 474

Brandl/Paffeneder, Datenschutzrechtliche Aspekte der Pay-As-You-Drive Versicherung, in Jahnel (Hrsg), Datenschutzrecht. Jahrbuch 2014 (2014) 191

Dammann/Simitis, EG-Datenschutzrichtlinie

Dohr/Pollirer/Weiss/Knyrim, DSG 2000. Datenschutz[2], 62.

Dörnhöfer, Datenschutz bei Grenzüberschreitungen. Zur Anwendbarkeit des DSG 2000 in grenzüberschreitenden Konstellationen, in Jahnel (Hrsg), Datenschutzrecht und E-Government. Jahrbuch 2012 (2012) 59.

Ennöckl, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung, in Raschauer (Hrsg) Forschung aus Staat und Recht 174

FIA Federation Internationale de l'Automobile, Technical Study, MyCarMyData

Hansen, Das Netz im Auto & das Auto im Netz, DuD 2015, 367

Jahnel, Datenschutzrecht in der Praxis, 14.

Jahnel, Datenschutzrecht

Judikatur
Datenschutzkommission K121.245/0009-DSK/2007
Datenschutzkommission K211.413/006-DSK/2002
OGH 19.11.2002, 4 Ob 179/02f
OGH 20.03.2007, 4 Ob 221/06p
VsSlg 16.369/2001
Verwaltungsgericht Köln, 11.11.2015, 21 K 450/15

Kipker, Privacy by Default und Privacy by Design, DuD 2015, 410

Knyrim, Datenschutzrecht[3]

Pachinger, Datenschutzrechtliche Fragen zu Mobilitätsdaten, ZIIR 2015, 266

Rost/Bock, Privacy By Design und die Neuen Schutzziele, DuD 2011, 30

Stratil (Hrsg), TKG 2003[4]

Unger, Grundzüge des Datenschutzrechts[2]

Weichert, Datenschutz im Auto, Das Kfz als großes Smartphone mit Rädern, SVR 2014, 201

Weisser/Färber, Rechtliche Rahmenbedingungen bei Connected Car
Überblick über die Rechtsprobleme der automobilen Zukunft, MMR 2015, 506

Online

Datum der letzten Abfrage: 15.03.2016

Allianz, Besondere Bedingung Pay As You Drive (PAYD) – „Fahr und Spar" – Tarif <https://www.allianz.at/v_1438676973000/firmenkunden/produkte/dokumente/BesBed_Fahr_und_Spar.pdf>

Apple Inc. <http://www.apple.com/ios/carplay/>

Art-29-Datenschutzgruppe, Stellungnahme 15/2011 der zur Definition von Einwilligung, WP 187, 34. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf>

Art-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, 01248/07/DE
<ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf>

Art-29-Datenschutzgruppe, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, 0829/14/DE <ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf>

Asfinag <http://www.asfinag.at/maut/vignette/digitale_vignette>

Der Standard, „Die Gefahr ist real": Auto-Hacks schrecken Branche auf

<http://derstandard.at/2000022195679/Die-Gefahr-ist-real-Auto-Hacks-schrecken-Branche-auf>

Europäischer Rat zur Datenschutzreform
<http://www.consilium.europa.eu/de/policies/data-protection-reform/>

Futurezone, Forscher hacken Corvette mittels SMS <http://futurezone.at/digital-life/forscher-hacken-corvette-mittels-sms/146.458.778>

Golem, ADAC fordert Ausschaltknopf für Datentransfers
<http://www.golem.de/news/vernetztes-fahren-adac-fordert-ausschaltknopf-fuer-datentransfers-1602-119372-2.html>

Google Inc. <https://www.android.com/auto/>

Hitachi Data Systems, The Internet on Wheels and Hitachi, Ltd. White Paper, November 2014
<http://www.hds.com/assets/pdf/hitachi-white-paper-internet-on-wheels.pdf>

Horz, Car2Car Kommunikation, 3. <https://www.uni-koblenz-landau.de/de/koblenz/fb4/ist/AGZoebel/Lehre/sommer2013/SeminarASidA/Horzz>

IT-Wissen, Das große Online-Lexikon für Informationstechnologie
<http://www.itwissen.info/definition/lexikon/V2X-vehicle-to-x.html>

Statistik Austria, Kfz-Bestand 2015
<http://www.statistik.at/wcm/idc/idcplg?IdcService=GET_PDF_FILE&RevisionSelectionMethod=LatestReleased&dDocName=107010>

Stepanek: „Jedes Auto produziert 10 GB Daten pro Stunde“, Futurezone, 29.04.2013 <http://futurezone.at/science/jedes-auto-produziert-10-gb-daten-pro-stunde/24.595.665>

wallstreet:online < http://www.wallstreet-online.de/aktien/alphabet-c-aktie/bilanz>

Wired; Hackers Remotely Kill a Jeep on the Highway—With Me in It
<http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

VII. Abkürzungsverzeichnis

Abs	Absatz
ADAC	Allgemeiner Deutscher Automobil-Club
AES	Advanced Encryption Standard
Anm	Anmerkung
C2C	Car to Car (Kommunikation zwischen 2 oder mehreren Fahrzeugen)
C2G	Car to Grid
C2P	Car to Pedestrian
C2R	Car to Roadside
C2X	Kommunikation zwischen dem Fahrzeug und der Umgebung
DSAV	Datenschutzangemessenheits-Verordnung
DSB	Datenschutzbehörde
DSG 2000	Datenschutzgesetz 2000
DS-GVO	Datenschutz Grundverordnung
DSK	Datenschutzkommission
DuD	Datenschutz und Datensicherheit
DVR	Datenverarbeitungsregister
eCall	Emergency Call
EDV	Elektronische Datenverarbeitung
ErwGr	Erwägungsgrund
EU	Europäische Union
FIA	Federation Internationale de l'Automobile
GB	Gigabyte
GSM	Global System for Mobile Communications
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
iSd	im Sinn des

leg cit	legis citatae
lit	litera
LTE	Long Term Evolution
M2M	Machine to Machine
MAC	Media Access Control
mE	meines Erachtens
MMR	Multimedia und Recht Zeitschrift für Informations-, Telekommunikations- und Medienrecht
MSD	Minimal Set of Data
OBU	On Board Unit
Opt	Opting
PIN	Persönliche Identifikationsnummer
RFID	radio-frequency identification
RL	Richtlinie
Rz	Randziffer
SSL	Secure Sockets Layer
SVR	Straßenverkehrsrecht, die Zeitschrift für die Praxis des Verkehrsjuristen
TKG	Telekommunikationsgesetz 2003
ua	unter anderem
UMTS	Universal Mobile Telecommunications System
uU	unter Umständen
vllt.	vielleicht
VO	Verordnung
WLAN	Wireless Local Area Network
z.B.	zum Beispiel
zw	Zwischen