Datenschutz-Grundverordnung im Automobilbereich

16.03.2017

Ass. iur. Rasmus Robrahn

uld65@datenschutzzentrum.de

Sitzung AK „Datensicherheit im Automobil“
des Zentralverbandes der Elektroindustrie

SeDaFa
Selbstdatenschutz im vernetzten Fahrzeug

iKoPA

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Gliederung

1. Warum Datenschutzrecht?
2. Allgemeines zur DSGVO
3. Ausgewählte Kernregelungen der DSGVO
4. Technischer und organisatorischer Datenschutz in der DSGVO
5. Standard-Datenschutzmodell
6. Ausblick auf die ePrivacy-Verordnung

Warum Datenschutzrecht?

- Volkszählungsurteil des BVerfG: Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

- Art. 8 Grundrechtecharta: Recht auf Schutz personenbezogener Daten

Allgemeines zur DSGVO

- VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

- 173 Erwägungsgründe (EG) und 99 Artikel (Art.)

Allgemeines zur DSGVO

- Ist bereits in Kraft getreten, gilt aber (erst) ab dem 25. Mai 2018
- Verordnung gilt im Gegensatz zur Richtlinie unmittelbar, kein Umsetzungsakt durch die Mitgliedsstaaten erforderlich
- Ziele der DSGVO
  - Harmonisierung des Datenschutzrechts in der EU
  - Modernisierung des Datenschutzrechts
  - Wettbewerbsangleichung

Kernregelungen der DSGVO

- Verbot mit Erlaubnisvorbehalt

  Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine Einwilligung vorliegt, oder die Voraussetzungen einer Rechtsgrundlage erfüllt sind.

Kernregelungen der DSGVO

- Personenbezogene Daten:

  „Im Sinne dieser Verordnung bezeichnet der Ausdruck: 1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen […]“, Art. 4 DSGVO

Kernregelungen der DSGVO

- Personenbezug bei vernetzten Fahrzeugen
  - Gemeinsame Erklärung vom Verband der Automobilindustrie und den Datenschutzbehörden: Jedenfalls dann personenbezogen, wenn Daten mit Kennzeichen oder Fahrzeugidentifikationsnummer verknüpft sind.
  - In Fahrzeugen befinden sich Menschen, bzw. jemand steuert das Fahrzeug
  - Driver Fingerprinting
  - Positionsdaten können sich auch aus gemessenen Geschwindigkeiten + Startpunkt ergeben

Kernregelungen der DSGVO

- Verarbeitungsgrundsätze, Art. 5 DSGVO
  - Rechtmäßigkeit
  - Verarbeitung nach Treu und Glauben
  - Transparenz
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit
  - Speicherbegrenzung
  - Integrität
  - Vertraulichkeit
  - Rechenschaftspflicht

Kernregelungen der DSGVO

- Rechte der betroffenen Person
  - Transparente Kommunikation
  - Information
  - Auskunft
  - Recht auf Berichtigung
  - Recht auf Löschung („Recht auf Vergessenwerden“)
  - Recht auf Einschränkung der Verarbeitung
  - Recht auf Datenübertragbarkeit

Kernregelungen der DSGVO

- Geldbußen
- Allgemeine Bedingungen für die Verhängung von Geldbußen
  - Immer Einzelfallbetrachtung, aber vorgegeben, was zu berücksichtigen ist (Art. 83 Abs. 2 DS-GVO)
    - Z.B.: Art, Schwere und Dauer des Verstoßes, Anzahl der von der Verarbeitung betroffenen Personen, vorsätzliches oder fahrlässiges Handeln, frühere Verstöße
  - Geldbußen sollen
    - wirksam
    - verhältnismäßig
    - abschreckend

    sein.
- Bis zu 20 000 000 Euro oder 4% des gesamten weltweit erzielten Vorjahresumsatzes, je nachdem, welcher Betrag höher ist.
- Strafrechtliche Folgen werden durch Mitgliedsstaaten geregelt

Technischer und organisatorischer Datenschutz in der DSGVO

- Art. 24 und 25 DSGVO regeln Datenschutz durch Technik
  - Privacy by Design
  - Privacy by Default

- Art. 32 DSGVO regelt IT-Sicherheit

Technischer und organisatorischer Datenschutz in der DSGVO

- Art. 24 und 25 DSGVO: Datenschutz durch Technikgestaltung
- Art. 25 DSGVO: Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung also auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen […], die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Technischer und organisatorischer Datenschutz in der DSGVO

- Ziel: Schutz der betroffenen Personen durch angemessenes Schutzniveau
- Herausforderungen:
  - Keine konkreten Vorgaben
  - Umfangreiche Abwägung notwendig

Technischer und organisatorischer Datenschutz in der DSGVO

- Art. 32 DSGVO Sicherheit der Verarbeitung
  - Ziel: Angemessenes Schutzniveau
  - Berücksichtigung des Risikos der Verarbeitung, des Stands der Technik, der Implementierungskosten, der Art, des Umfangs und der Umstände und Zwecke der Datenverarbeitung
  - Beispielhafte Nennung von „Maßnahmen“
    - Pseudonymisierung, Verschlüsselung
    - Sicherung von Vertraulichkeit, Integrität, Verfügbarkeit und Robustheit
    - Regelmäßige und systematische Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen

Standard-Datenschutzmodell

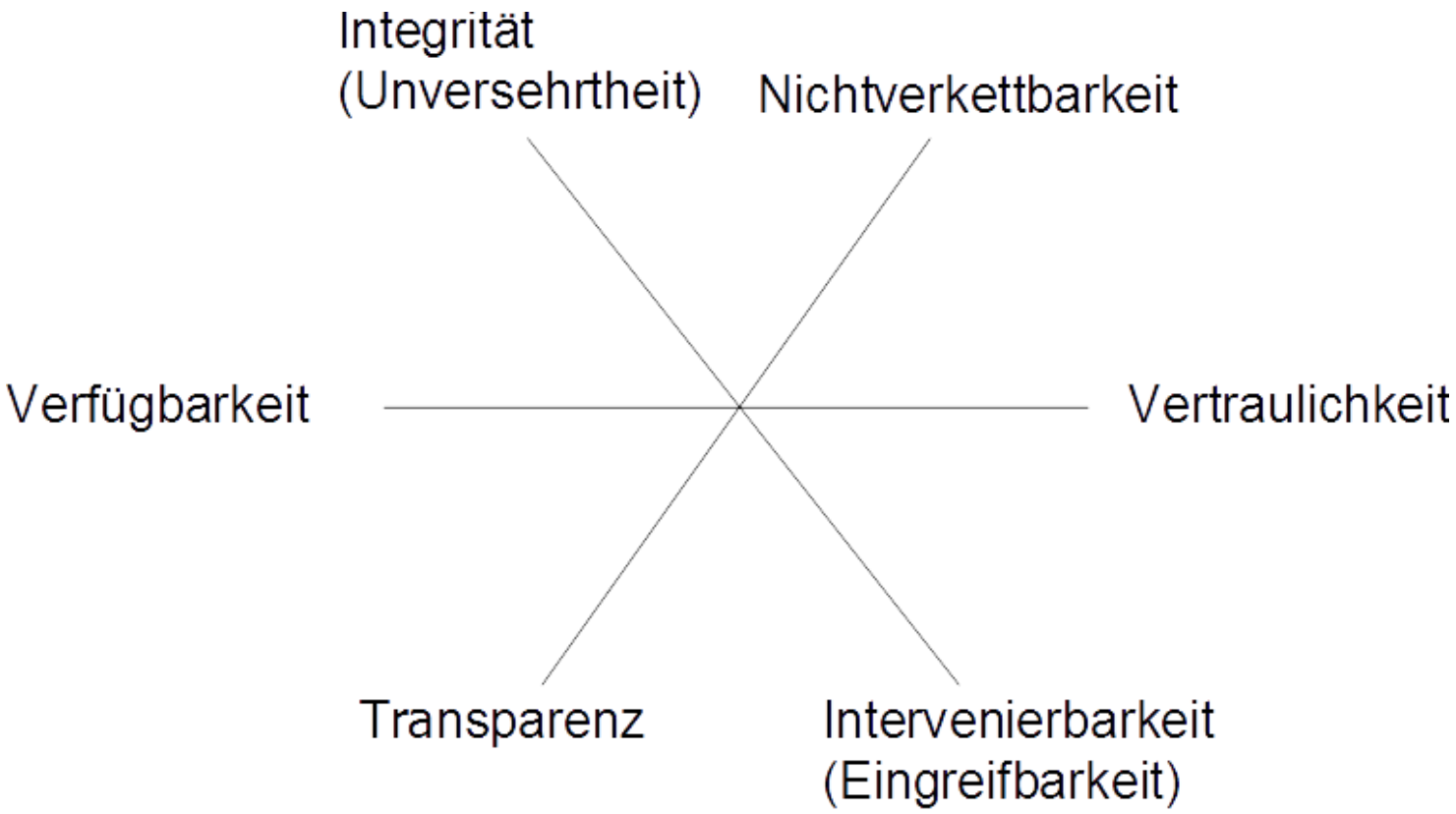
- Prüf- und Beratungsmethodik der Datenschutzbeauftragten des Bundes und der Länder
- V.1.0 von der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 9. und 10. November 2016 in Kühlungsborn einstimmig zustimmend zur Kenntnis genommen (Enthaltung durch Freistaat Bayern)
- Englische Version seit dem 01.03.2017 veröffentlicht.
- www.datenschutzzentrum.de/sdm

Standard-Datenschutzmodell

- Ziele des SDM:
  - Abstrakte rechtliche Regelungen in konkrete Maßnahmen überführen
  - Strukturierung der Anforderungen
  - Schutz der betroffenen Personen
- Die Elemente des SDM:
  - Schutzziele
  - Schutzbedarf
  - Verfahren
  - Maßnahmenkatalog

Standard-Datenschutzmodell

- 6 Schutzziele + Datenminimierung



Standard-Datenschutzmodell

- Schutzziele
  - Datenminimierung
    - Es sollen nicht mehr Daten erhoben, verarbeitet und genutzt werden, als für das Erreichen des Verarbeitungszweckes erforderlich ist.
  - Vertraulichkeit
    - Es kann nicht unbefugt Kenntnis von personenbezogenen Daten genommen werden.
  - Verfügbarkeit
    - Personenbezogene Daten stehen zur Verfügung und müssen verwendet werden können.
  - Integrität
    - Die Spezifikationen des Systems werden eingehalten. Personenbezogene Daten können nicht unbefugt verändert werden.

Standard-Datenschutzmodell

- Schutzziele
  - Nichtverkettbarkeit
    - Daten können nur für den Zweck verarbeitet werden, für den sie erhoben wurden.
  - Transparenz
    - Betroffene, Verantwortliche und Aufsichtsbehörden können erkennen, welche Daten wie verarbeitet werden.
  - Intervenierbarkeit
    - Die Betroffenenrechte (Information, Auskunft, Berichtigung, Einschränkung, Datenübertragbarkeit und Löschung) werden wirksam gewährt.

Standard-Datenschutzmodell

- Verfahren
  - Daten
  - Systeme
  - Prozesse

Standard-Datenschutzmodell

- Schutzbedarf
  - Drei Stufen: normal, hoch, sehr hoch
  - Schutz des Betroffenen
  - Es geht nicht um klassische Risikobetrachtung (Risiko = Eintrittswahrscheinlichkeit x Schaden)

Standard-Datenschutzmodell

- Schutzbedarf
  - Hoher Schutzbedarf, wenn es sich um ein Verfahren mit einer erhöhten Eingriffsintensität handelt.
    - Art der Daten
      - Z.B. Sensitive Daten
    - Vielzahl von betroffenen Personen
    - Vielzahl von Daten über einzelne betroffene Personen
    - Daten mit hoher Verknüpfbarkeit
    - Daten aus dem inneren Lebensbereich der betroffenen Personen

Standard-Datenschutzmodell

- Schutzbedarf bei vernetzten/datenverarbeitenden Fahrzeugen
  - Fahrzeug wird von vielen Bürgern täglich genutzt
    - Einblicke in den Alltag
  - Positionsdaten
  - Daten aus denen sich die Position ableiten lässt
  - Fahrerprofile
  - Daten können große Rolle in Gerichtsprozessen spielen

Standard-Datenschutzmodell

- Maßnahmenkatalog der Aufsichtsbehörden ist noch nicht fertig gestellt.
- Nachfolgende Maßnahmen sind Beispiele für das vernetzte Auto.

Standard-Datenschutzmodell

- Maßnahmen für **Transparenz**
  - Information des Nutzers durch das HMI
  - Informationen müssen auch für andere Fahrer als den Halter verfügbar sein
  - Welche Dienste sind aktiv?
  - Werden aktuell Daten übertragen?
  - Handelt es sich um pseudonyme, anonyme oder unmittelbar personenbezogene Daten?
  - Besondere Herausforderungen durch ganz unterschiedlicher Adressaten
    - Adressatengerechte Informationen

Standard-Datenschutzmodell

- Maßnahmen für **Intervenierbarkeit**
  - „Aus-Schalter"
  - Im Fahrzeug und im Backend befindliche Daten können von den Nutzern gelöscht werden
  - Konfigurierbarkeit der Datenverarbeitung, welche Funktionen möchte ich als betroffene Person nutzen und welche nicht?
  - Wie kann auf Mängel bei der Datenverarbeitung reagiert werden? Sind Updates möglich?
  - Einfache Geltendmachung der Betroffenenrechte (z.B. auch über HMI)
  - Privacy by Default: Voreinstellungen im Fahrzeug sollten datensparsam sein

Standard-Datenschutzmodell

- Maßnahmen für **Nichtverkettbarkeit** und Datenminimierung
  - Frühestmögliche Anonymisierung oder Pseudonymisierung
    - Anonymisierung ist der Pseudonymisierung vorzuziehen
    - Wechselnde Pseudonyme
  - Zentrale Entitäten in der Kommunikation vermeiden
  - Datenverarbeitungen für unterschiedliche Zwecke sind voneinander zu trennen
  - Datenschutzfördernde Attributbasierte Credentials
  - Wann können Daten gelöscht oder gesperrt werden?

Standard-Datenschutzmodell

- **Vertraulichkeit, Verfügbarkeit, Integrität**
  - Verschlüsselung
  - Richtigkeit von personenbezogenen Daten muss gewährleistet werden
    - Schutz vor unbefugter Modifikation
  - Vertraulichkeit gegenüber anderen Fahrern
  - Redundanzen

Ausblick auf die ePrivacy-Verordnung

- Soll ebenfalls ab dem 25. Mai 2018 gelten
- Kommissionsentwurf
  - Schutz bei elektronischer Kommunikation, nicht nur klassische Telekommunikation
  - Pflichten für Softwarehersteller
  - Starke Betonung der Einwilligung

Vielen Dank für die Aufmerksamkeit!
Fragen?

Selbstdatenschutz im vernetzten Fahrzeug

GEFÖRDERT VOM

funded by the
German Federal Ministry
of Education and Research

www.sedafa-projekt.de

integrierte
Kommunikationsplattform für
automatisierte Elektrofahrzeuge

GEFÖRDERT VOM

funded by the
German Federal Ministry
of Education and Research

https://fgvt.htwsaar.de/public
/index.php/ikopa-2015-2018/