MAYER·BROWN

Autonomes Fahren in Deutschland – Cybersecurity

Automotive

Ulrich Worm
Rechtsanwalt
T +49 69 7941 2981
uworm@mayerbrown.com

Mayer Brown is a global legal services provider comprising legal practices that are separate entities (the "Mayer Brown Practices"). The Mayer Brown Practices are: Mayer Brown LLP and Mayer Brown Europe-Brussels LLP, both limited liability partnerships established in Illinois USA; Mayer Brown International LLP, a limited liability partnership incorporated in England and Wales (authorized and regulated by the Solicitors Regulation Authority and registered in England and Wales number OC 303359); Mayer Brown, a SELAS established in France; Mayer Brown JSM, a Hong Kong partnership and its associated legal practices in Asia; and Tauil & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. Mayer Brown Consulting (Singapore) Pte. Ltd and its subsidiary, which are affiliated with Mayer Brown, provide customs and trade advisory and consultancy services, not legal services. "Mayer Brown" and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.

Einführung

- Welche rechtlichen Rahmenbedingungen gibt es für Cybersecurity bei autonomen und vernetzten Fahrzeugen?
- Welche gesetzgeberischen Maßnahmen sind auf deutscher und europäischer Ebene hierzu in naher Zukunft zu erwarten?
- Besondere Herausforderungen von Over-the-Air Updates
- Welche Vorsorgemaßnahmen sind angezeigt?

Gesetzliche Grundlagen (1)

- Was versteht man eigentlich unter Cybersecurity?
- Keine spezifische Gesetzgebung in Europa betreffend Cybersecurity für autonome und vernetzte Fahrzeuge
- Mit Ausnahme des BSI-Gesetzes und des IT-Sicherheitsgesetzes gibt es auch außerhalb dieses Bereichs kaum spezifische Gesetzgebung zum Thema Cybersecurity

Gesetzliche Grundlagen (2)

- Das BSI-Gesetz und das IT-Sicherheitsgesetz setzen die NIS Richtlinie um
- Regelungsgegenstand des BSI-Gesetzes und des IT-Sicherheitsgesetzes
- Kritis-VO „Transport und Verkehr“
- Straßenverkehr in Anhang 7, Teil 1 Nr. 1 lit.d) aufgeführt – betrifft allerdings nur Verkehrsleitsysteme aber keine (autonomen) Fahrzeuge

Gesetzliche Grundlagen (3)

- Telemediengesetz
  - Anwendbarkeit, § 1 Abs. 1 TMG
  - Enthält Sicherheitsanforderungen in § 13 Abs. 7 TMG
- Telekommunikationsgesetz
  - Anwendbarkeit, § 3 Nr. 24 TKG
  - Sicherheitsanforderungen, §§ 109 und 109a TKG für öffentlich zugängliche Telekommunikationsdienste
  - Technische Vorkehrungen zum Datenschutz und -geheimnis, § 109 Abs. 1 TKG
  - Vorkehrungen gegen Störungen und Angriffe, § 109 Abs. 2 TKG
  - Berücksichtigung des Standes der Technik
  - Sicherheitskonzept, § 109 Abs. 4 TKG
  - Meldepflichten, §§ 109 Abs. 5 und 109a TKG

Gesetzliche Grundlagen (4)

- Produktsicherheitsgesetz
- Datenschutz-Grundverordnung
  - Sachliche Anwendbarkeit: Nur personenbezogene Daten
  - Persönliche Anwendbarkeit: Jede Stelle, die mit der „Verarbeitung“ personenbezogener Daten beschäftigt ist, vgl. § 4(2) DSGVO
  - Privacy-by-Design und Privacy-by-Default, Art. 25 DSGVO
  - Integrität und Vertraulichkeit, Art. 5(1)(f) DSGVO
  - Technische und organisatorische Maßnahmen um angemessenes Sicherheitsniveau zu gewährleisten, Art. 32(1) DSGVO
  - Möglichkeit, branchenweite Verhaltensregegeln zu setzen, Art. 40 DSGVO

Gesetzliche Grundlagen (5)

- VDA „Datenschutzprinzipien für vernetzte Fahrzeuge“
- Auto-ISAC Best Practices
- Standard SAE J3061: “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems”
- Entwurf des Standards ISO/SAE AWI 21434: “Road Vehicles -- Cybersecurity engineering”
- ENISA Guide „Cybersecurity and Resilience of smart cars - good practices and recommendations”

Zu erwartende gesetzgeberische Maßnahmen (1)

- Aufnahme autonomer Fahrzeuge und sämtlicher Infrastruktureinrichtungen in die BSIG Kritis-VO?
  - Hierdurch entstünde u.a. Pflicht, Vorkehrungen zu ergreifen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der Systeme, § 8a Abs. 1 BSIG
  - Betreiber und Branchenverbände können Sicherheitsstandards vorschlagen, § 8a Abs. 2 BSIG
  - Nachweispflichten und Verpflichtung zur Duldung von Audits, § 8a Abs. 3 BSIG
  - Pflicht zur Risikovorsorge, § 8c Abs. 1 BSIG
  - Pflicht zur Berücksichtigung des Standes der Technik
- Derzeit jedoch keine kommunizierten Pläne hierzu

Zu erwartende gesetzgeberische Maßnahmen (2)

- Digital Single Market: Europäische Kommission plant Regelungen für nicht-personenbezogene Daten (*Communication from the Commission* vom 10. Mai 2017); Ziele:
  - Free flow of non-personal data
  - Rechtezuordnung
  - Cybersecurity
- E-Privacy Verordnung
  - Datenschutzrechliche und sicherheitstechnische Vorgaben

Zu erwartende gesetzgeberische Maßnahmen (3)

- EU Cybersecurity Act
  - Zertifizierungssystem
  - Cybersecurity Agency
  - Derzeitiger Entwurf enthält allerdings noch keine spezifischen Regelungen zum Thema autonome und vernetze Fahrzeuge
- Weitere denkbare gesetzliche Regelungen:
  - Pflicht zur Trennung von Systemen, welche für das autonome Verfahren von Bedeutung sind, von anderen Systemen (z.B. dem Infotainmentsystem)
  - Pflicht zur Anzeige des Softwarestandes und der ergriffenen Maßnahmen zum Schutz der Integrität der Systeme
  - Ausdrückliche Verpflichtung, zeitnah Updates aufzuspielen, um aktuellste Sicherheitsstandards zu gewährleisten

Besondere Herausforderungen von Over-the-Air Updates (1)

- Was sind Over-the-Air Updates?
  - Kabellose Updates
  - Vereinfachung von Updates
  - Freischaltung neuer Funktionen
  - Übermittlung von Sicherheitshinweisen oder Hinweisen auf Wartungstermine
  - Übermittlung von Warnhinweisen oder Rückrufaufforderungen

Besondere Herausforderungen von Over-the-Air Updates (2)

- Welche rechtlichen Implikationen ergeben sich aus (der Möglichkeit von) Over-the-Air Updates?
  - Produkthaftung
  - Produktsicherheit
  - Gewährleistungsrecht
  - Regulatorische Aspekte
  - Zivilrechtliche Aspekte

Angezeigte Vorsorgemaßnahmen (1)

- Selbstverständlich:
  - Entwürfe zum EU Cybersecurity Act, zur E-Privacy Verordnung und zum Digital Single Market verfolgen
  - Maßnahmen zum Privacy-by-Design und Privacy-by-Default ergreifen
  - Maßnahmen zum Security-by-Design und Security-by-Default ergreifen
  - Kritische Prüfung von Open Source Software Elementen
  - Insbesondere: Maßnahmen zur Vermeidung von Hackerangriffen ergreifen
  - Umfassende Dokumentation der ergriffenen Maßnahmen

Angezeigte Vorsorgemaßnahmen (2)

- Welche Maßnahmen sind zu ergreifen im Hinblick auf unausweichliche „Störfälle“?
  - Simulationen von Ernstfällen
  - Cyber Incident Response Plans
  - Cybersecurity Versicherungen

Ihr Ansprechpartner

Dr. Ulrich Worm

Partner, Frankfurt am Main
Intellectual Property
uworm@mayerbrown.com
T +49 69 7941 2981