

# PRIVACY BY DESIGN: EINE GEMEINSAME HERAUSFORDERUNG VON IT, INGENIEUREN UND MANAGERN ZUR EFFEKTIVEN UMSETZUNG DES DATENSCHUTZRECHTS

Ein Anwendungsfall am Beispiel des autonomen Fahrzeugs

**Sheila Vásquez, LL.M.**

Universität Oldenburg

Herbstakademie 2021

# Überblick

1. Einleitung
2. Privacy by Design und das autonome Fahrzeug
3. Rechtsentwicklung
4. Die StVG-Novelle und die DSGVO
5. Organisatorische Maßnahmen
6. Fazit

# Das neue Gesetz zum autonomen Fahren

|  |                       |        |
|--|-----------------------|--------|
| <b>Bundesrat</b>   | Drucksache            | 155/21 |
|  | 12.02.21              |        |
|  | Vk - Fz - In - K - Wi |        |
| <b>Gesetzentwurf</b><br>der Bundesregierung  |                       |        |
| <b>Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes - Gesetz zum autonomen Fahren</b>  |                       |        |
| <b>A. Problem und Ziel</b>   |                       |        |
| Die Entwicklungsdynamik im Bereich des automatisierten, autonomen und vernetzten Fahrens ist ungebrochen hoch. Um die Potenziale dieser Technologien heben zu können und die Teilhabe der Gesellschaft daran zu ermöglichen, bedarf es der Umsetzung weiterer Schritte zur Einführung entsprechender Systeme in den Regelbetrieb. Anknüpfend an die bisherigen rechtlichen Vorgaben des Achten Gesetzes zur Änderung des Straßenverkehrsgesetzes zum Betrieb von Kraftfahrzeugen mit hoch- und vollautomatisierter Fahrfunktion stellt sich die Notwendigkeit dar, über die im öffentlichen Straßenverkehr bereits mögliche Erprobung autonomer, führerloser Fahrzeuge hinauszugehen und deren Regelbetrieb einzuleiten. Zunächst sollen autonome Fahrzeuge dafür in festgelegten Betriebsbereichen eingesetzt werden können. Mangels internationaler, harmonisierter Vorschriften bedarf es bei derart weitreichenden technischen Entwicklungen Regelungen des Gesetzgebers zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion sowie zu den Anforderungen an die Beteiligten und an das Kraftfahrzeug selbst. |                       |        |
| Auch Fahrzeuge der Bundeswehr, der Bundespolizei, der Landespolizei, des Zivil- und Katastrophenschutzes, der Feuerwehren und Rettungsdienste nutzen autonome Funktionen. Diese Fahrzeuge unterliegen jedoch in ihrem Einsatzspektrum besonderen Betriebsbedingungen und haben besondere Ausstattungen, für die die Erteilung der Betriebserlaubnis im Eigenvollzug weiterhin möglich sein muss.   |                       |        |
| <b>B. Lösung</b>   |                       |        |
| Ein geeigneter Rechtsrahmen soll durch Ergänzung bestehender Regelungen des Straßenverkehrsrechts geschaffen werden. Nach geltendem Recht können autonome Kraftfahrzeuge im öffentlichen Verkehr betrieben werden, sofern diese Fahrzeuge und deren jeweilige Betriebsbereiche für die jeweiligen Fahrzeuge durch die zuständigen Behörden genehmigt worden sind.  |                       |        |
| Bisher gibt es auf europäischer Ebene keinen hinreichenden Rechtsrahmen für Kraftfahr-   |                       |        |
| Fristablauf: 26.03.21  |                       |        |

- ▶ **Das neue Gesetz zum autonomen Fahren führt zu einer Novellierung des Straßenverkehrs- und Pflichtversicherungsgesetzes**
- ▶ **Der Gesetzgeber schafft mit § 1g StVG Datenverarbeitung (neu) Halterpflichten zur Datenspeicherung und adressiert dabei die Hersteller: Sie sollen hinsichtlich der Verarbeitung von Daten „in der Software des Kraftfahrzeugs“ dem Halter „entsprechende Einstellungen ermöglichen“**
- ▶ **In der Begründung zu § 1g Abs. 3 StVG heißt es: „hiermit wird auch dem Grundsatz des „Privacy by Design“ Rechnung getragen“**

## Fokus der Arbeit



### Untersuchungsgegenstand und Fragestellungen



*Welche Funktion kann Privacy by Design im Zusammenhang mit autonomen Fahrzeugen erfüllen?*



*Welche Anforderungen bezüglich Privacy by Design können aus Art. 25 DSGVO "Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen" abgeleitet werden?*



*Ist Privacy by Design ausschließlich eine Aufgabe der Technikgestaltung?*

## 2. Privacy by Design und das autonome Fahrzeug

## Privacy by Design: Definition und Abgrenzung

- **„Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ = Data Protection by Design and by default (Art. 25 DSGVO)**
  - Der Verantwortliche ist verpflichtet zum Einsatz von geeigneten technischen und organisatorischen Maßnahmen, um die Datenschutzgrundsätze gemäß Art. 5 DSGVO in der Gestaltung risikoadäquat und effektiv umzusetzen
  
- **Der Grundsatz „Privacy by Design“ berücksichtigt hinsichtlich der datenschutzrechtlichen Gestaltung von Technologie auch ethische Aspekte** in Übereinstimmung mit der Grundrechtecharta der Europäischen Union (EDSB, Leitlinie 5/2018)

## Das autonome Fahrzeug als Anwendungsfall

- 👁️ **Ausgangslage:** Das autonome Fahrzeug bietet einen zukünftigen Mehrwert für die Gesellschaft:
  - Erhöhung der Verkehrssicherheit (Reduzierung des menschlichen Fehlverhaltens) & Entlastung des Fahrers
- ⚡ **Herausforderung:** Damit das autonome Fahrzeug sich auf dem Markt durchsetzt, sind jedoch Akzeptanz und Vertrauen der Nutzer in diese neue Technologie notwendig
  - 70 % der Befragten sehen Hacker-Angriffe als Risiko /
  - 60 % der Befragten haben Angst bei der Nutzung dieser neuen Technologie überwacht zu werden



*Privacy by Design könnte bei der datenschutzrechtlichen konformen Gestaltung von Technologie eine besondere Rolle spielen zur Steigerung des Vertrauens in das autonome Fahrzeug*

Quelle: <https://de.statista.com/statistik/daten/studie/1035382/umfrage/umfrage-zu-hindernisgruenden-bei-nutzung-autonomer-fahrzeuge/>  
<https://de.statista.com/statistik/daten/studie/270612/umfrage/nachteile-von-autonomen-fahrzeugen/>

## 3. Rechtsentwicklung



# Unterschiedliche internationale Entwicklung des Privacy by Design



## Privacy by Design

- Datenschutz durch **Technikgestaltung**
- Systemdatenschutz



## Privacy by Design

- Data Protection by Design
- Privacy-enhancing Technologies (PET)



## Privacy by Design

- Vgl. The 7 Foundational Principles

## Vergleich der lokalen Überschrift des Art. 25 DSGVO

 Datenschutz durch Technikgestaltung



 Data protection by **design (EN)**

 Protección de datos desde el **diseño**

 Protection des données dès la **conception**



***Prinzip:** Die Datenschutzgrundsätze sollten „eingebaut“ bzw. im Rahmen der „Gestaltung“ berücksichtigt werden*



## 3. Rechtsentwicklung

- ⚡ **Herausforderung:** Offen bleibt die Konkretisierung der technischen und organisatorischen Maßnahmen
  - **Durch die daraus resultierende Rechtsunsicherheit entsteht ein Ermessensspielraum** in der Berücksichtigung der Bedürfnisse des Verantwortlichen
  - **Für die Betroffenen könnte dies zu Risiken für ihre Rechte und Freiheiten führen und im konkreten Fall des autonomen Fahrzeugs zu einem reduzierten Vertrauen** in die Nutzung dieser neuen Technologie

Mit der StVG-Novelle hat der Gesetzgeber nun auch außerhalb der technologieneutralen Datenschutzgesetze für eine konkrete Technologie (das autonome Fahrzeug) einen Bezug zu Privacy by Design hergestellt

## 4. Die StvG-Novelle und die DSGVO

## Die StVG-Novelle und die DSGVO: Halterpflichten

**§ 1g Abs. 1 StVG:** „Der Halter eines Kraftfahrzeugs mit autonomer Fahrfunktion ist verpflichtet folgende Daten beim Betrieb eines Kraftfahrzeugs mit autonomer Funktion zu speichern“

- **Der Halter wird zum Verantwortlichen i.S.d. Art. 4 Nr. 7 DSGVO**
- **Es ergibt sich für die Rechtmäßigkeit der Verarbeitung § 1g Abs. 1 StVG eine rechtliche Verpflichtung im Sinne des Art. 6 Abs. 1 lit. c DSGVO**

## Die StVG-Novelle und die DSGVO: Herstellerpflichten

**§ 1g Abs. 3 StVG:** „Der Hersteller muss den Halter präzise, klar und in leichter Sprache über die Einstellungsmöglichkeiten zur Privatsphäre und zur Verarbeitung der Daten informieren, die beim Betrieb des Kraftfahrzeugs in der autonomen Fahrfunktion verarbeitet werden. Die diesbezügliche Software des Kraftfahrzeugs muss dem Halter entsprechende Einstellungen ermöglichen.“

- **Gesetzesbegründung zu § 1g Abs. 3 StVG:** „Hiermit wird auch dem Grundsatz des „Privacy by Design“ Rechnung getragen“



Gemäß **ErwG 78 DSGVO** wird der „Hersteller“ zur Einhaltung von Art. 25 DSGVO „ermutigt“

## 5. Organisatorische Maßnahmen

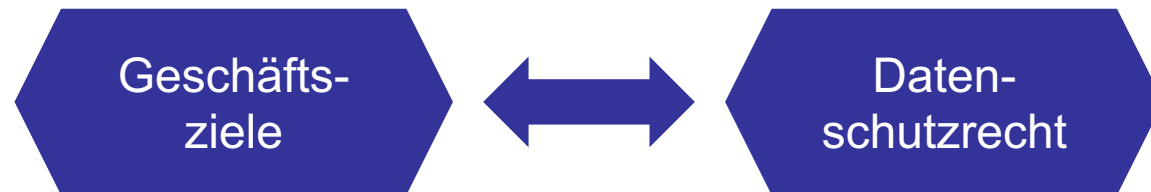
## Organisatorische Maßnahmen: Überblick

- **Die Etablierung des Privacy by Design war – vom Datenschutz durch Technik und Systemdatenschutz ausgehend – bislang stark auf die technisch gestützte Gestaltung ausgelegt**
- **Die Beschränkung des Data Protection by Design auf die Technik bzw. technische Maßnahmen ist vom Gesetzgeber nicht beabsichtigt**



## Organisatorische Maßnahmen: Prozesse und Rollen

- **Organisatorische Maßnahmen sollten im Kontext der Definition der Mittel und Zwecke der Verarbeitung berücksichtigt werden** – hier spielt neben den technischen Ansprechpartnern des Unternehmens, wie IT und Ingenieuren, auch das Management eine wichtige Rolle
- **Bereits in der Frühphase der Entwicklung sollten strategische Fragen berücksichtigt werden**, z.B. die Frage der Datenhoheit, der Datenverfügbarkeit und die mit ihr verbundene Zentralisierung oder Dezentralisierung eines Systems zur Verarbeitung personenbezogener Daten



## Organisatorische Maßnahmen: Transparenz

### Herausforderung:

- Vernetzte Fahrzeuge können Nutzer angesichts der Vielfalt an Informationen überfordern
- Folglich kann das Recht auf informationelle Selbstbestimmung gefährdet werden

### Lösung:

- **Gestaltung intelligenter Datenschutzkonzepte im Fahrzeug**  
bspw. User-Onboarding
- **Einführung von Standardisierungsprozessen für die Definition von Piktogrammen**, welche z.B. im Fahrzeug, Apps und Websites einheitlich angezeigt werden
- **Management Aufgabe: Eine Standardisierung und die notwendigen Prozesse dafür zu schaffen**

## Organisatorische Maßnahmen: Ressourcen

- **Es sollte sichergestellt werden, dass für die Implementierung der geeigneten technischen und organisatorischen Maßnahmen notwendige Ressourcen frühzeitig eingeplant werden**
- **Im Unternehmen erfolgt die Ressourcenplanung unter Einbindung des Managements** und verbleibt nicht als rein technische Aufgabe
- **Auch die Qualifizierung von Personal bedarf der Ressourcenplanung zugunsten einer effektiven Implementierung.** Ferner ist die Ressourcenplanung für den Einsatz von genehmigten Zertifizierungsmaßnahmen i.S.d. Art. 42 DSGVO notwendig, welche für den Nachweis des Einhaltens der Anforderungen aus Art. 25 DSGVO dienen

## 6. Fazit

## Fazit

1

Privacy by Design kann als der Datenschutzgrundsätze integrierende Prozess betrachtet werden, welcher sowohl technische, als auch organisatorische Komponenten berücksichtigen sollte

2

Die Verpflichtung von Herstellern zum Privacy by Design in § 1g StVG ist ein wichtiger Schritt, um mehr Vertrauen in diese neue Technologie zu schaffen

3

Es fehlt jedoch an Konkretisierung, insbesondere im Hinblick auf die organisatorischen Maßnahmen, welche auch eine Aufgabe des Managements sind



**Vielen Dank für Ihre  
Aufmerksamkeit!**