Prof. Dr. Andreas Wiebe, LL.M. (Virginia)
Obmann Forschungsverein Infolaw
Lehrstuhl für Bürgerliches Recht,
Wettbewerbs- und Immaterialgüterrecht,
Medien- und Informationsrecht,
Universität Göttingen

18. Öst. IT-Rechtstag
Wien

# Der Data Act – Innovation durch Zugangsrechte?

25. April 2024

# Übersicht

- Das Ökosystem des Datenrechts
- Vom "Dateneigentum" zu Zugangsrechten
- Data Act
  - Sachlicher Anwendungsbereich
  - Rollenverteilung
  - Zugangsrechte
  - Das nutzerzentrierte Modell des DA
  - Bereitstellung von Daten an Empfänger
  - Datenzugang und Geheimnisschutz im Konflikt
  - Datenzugang und Datenschutzrecht
  - Grenzüberschreitendes Datenrecht
- Sektorspezifische Regelung am Bsp. Connected Car
  - Sektorspezifische Zugangsregeln
  - Weitere Regulierungsnotwendigkeiten
- Fazit

# Das Ökosystem des Datenrechts

- DSGVO
- Digitale-Inhalte-Richtlinie (DI-RL) – Vertragsrecht digitaler Produkte
- Open-Data-RL (insb. Art. 13, 14 OD-RL) – Weiterverwendung bei Behörden gespeicherter Daten
- P2B-VO 2019/1150 – Fairness und Transparenz ür gewerbliche Nutzer auf Online-Plattformen
- Digital Markets Act (‚Gatekeeper') – Kartellrecht für große Digitalunternehmen
- Digital Services Act (‚Vermittlungsdienste') – Rahmen für digitale Dienste
- Data Governance Act - insb. Ermöglichung von Datenvermittlungsdiensten
- **Data-Act – Zugang zu Daten bei vernetzten Produkten**
- KI-Regulierung
  - AI Act KOM (2021)206 endg v. 21.4.2021– Rahmen für Entwicklung von KI-Systemen, EP Legislative Resolution Mach 13, 2024
  - ProdHaftRL KOM(2022) 495 endg. v. 28.9.2022– Haftung für KI als Produkt
  - KI-Haftungs-RL KOM(2022) 496 endg v. 28.9.2022– Haftung für Verletzung AI Act
- CoC, zB Landwirtschaft, EU Code of Conduct on Agricultural Data Sharing 2018
- „Data Spaces", zB Health Data Space VO
- A European Strategy for Data, COM(2020) 66 final

# Vom "Dateneigentum" zu Zugangsrechten

- De lege lata: kein immaterialgüterrechtlicher Schutz von Daten
  - Urheberrecht: kein Schutz für Daten an sich, nur bei Werkeigenschaft
  - Datenbankherstellerrecht: Schutz von Daten, die ausgeschützter Datenbank
  - Analogie zum zivilrechtlichen Eigentum nicht tragfähig (Variationen DACH)
  - Deshalb idR. relativer Schutz durch Geheimnisschutz und StGB -> rechtlicher Schutz des Zugangs zu und der Integrität von Daten

- Rechtspolitische Diskussion
  - Communication Building a European data economy, COM(2017) 9 final v. 10.1.2017
    - Datenproduzentenrecht oder Sui-generis-Abwehrrecht?
    - Probleme: Abgrenzung Schutzgegenstand, "Super-IP", Zuordnung

  -> Zugangsrechte

# Vom "Dateneigentum" zu Zugangsrechten

Ziel: Data Sharing zur Förderung von Innovation
- Ausgangspunkt: faktische Kontrolle, Informationsdilemma
- Spannungsfeld: Anreiz zur Informationsproduktion ./. Verbreitung von Daten
- bei nicht-personenbezogenen Daten: freier Zugang zu Daten wünschenswert (Nichtrivalität der Nutzung)
- OECD: Information als Infrastruktur
- iÜ: technische Schutzmaßnahmen möglich

Funktion der faktischen Ausschließlichkeit
- (-): behindert Entstehen von Märkten
- (+): Vertragsgrundlage, durch Vertragsrecht kontrollierte Offenbarung möglich

→ Datenzugangsrechte + Datenverträge als geeignete Instrumente

Erwgrd 2 DA: „optimale Verteilung der Daten zum Nutzen der Gesellschaft"

# Data Act – VO 2023/2854 v. 13.12.2023

Sachlicher Anwendungsbereich

- „Vernetztes Produkt“: Gegenstand, der Daten über seine Nutzung oder Umgebung erlangt, generiert oder erhebt und der Produktdaten über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang übermitteln kann …;
  - Autos, Haushaltsanlagen, Verbrauchsgüter, Gesundheitsgeräte, industrielle/Agrarmaschinen
  - Rohdaten und “aufbereitete Daten”
  - Nicht aus den Daten gefolgerte oder abgeleitete Informationen (Erwgrd 15)
- Produkte, die vornehmlich dem Anzeigen oder Aufnehmen von Inhalten dienen und daher menschlichen Input benötigen, sind nicht abgedeckt (personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners)

# Data Act – VO 2023/2854 v. 13.12.2023

- Rollenverteilung

„Dateninhaber“

eine natürliche oder juristische Person, die nach Unionsrecht …berechtigt oder verpflichtet ist, Daten …zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat;

„Nutzer“

eine natürliche oder juristische Person, die ein vernetztes Produkt besitzt oder der vertraglich zeitweilige Rechte für die Nutzung des vernetzten Produkts übertragen wurden oder die verbundenen Dienste in Anspruch nimmt;

„Datenempfänger“

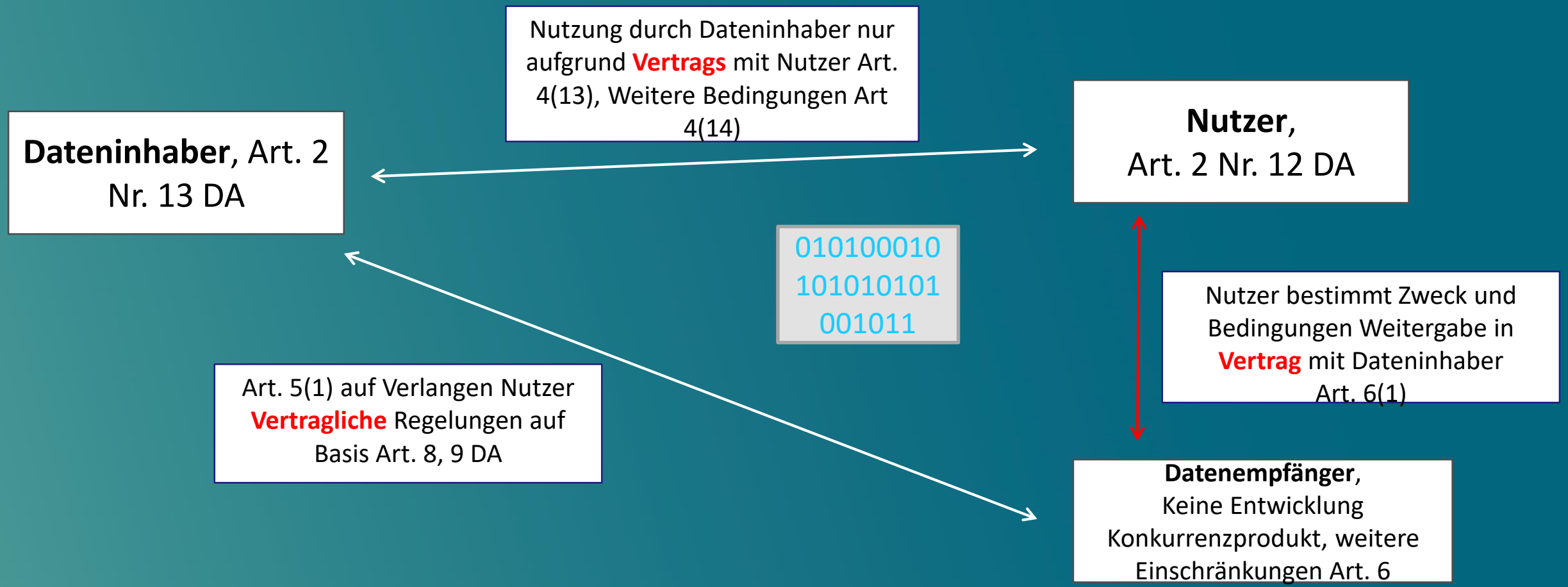
Person, die zu gewerblichen oder beruflichen Zwecken handelt, und der vom Dateninhaber Daten bereitgestellt werden, einschl. eines Dritten, dem auf Verlangen des Nutzers die Daten bereitgestellt werden.

# Data Act – VO 2023/2854 v. 13.12.2023

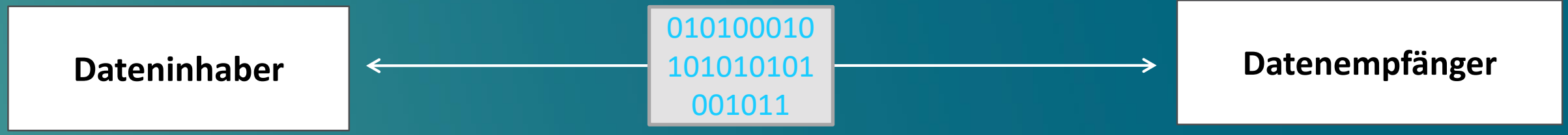
Zugangsrechte

- Nutzer
  - Art. 3 – Zugang Teil des Produktdesigns
  - Art. 4 – Anspruch auf Zugang zu Daten, direkt, in Echtzeit, in-situ-Access auf Verlangen Nutzer
- Dritter
  - Art. 5 – Weitergabe an Dritte durch Dateninhaber auf Verlangen Nutzer

# Das (nutzerzentrierte) Modell des Data Act



# Bereitstellen von Daten an Datenempfänger




**FRAND**, Art. 8 I DA

Kap. III, IV DA-E, genauer Inhalt ?

Angemessene **Gegenleistung**, Art. 9

Gewinnspanne, Kosten für Bereitstellung und Produktion der Daten

**Einschränkungen Art. 6**

Zweckbindung für Nutzung und Weitergabe, kein Konkurrenzprodukt, keine Weitergabebindung Nutzer

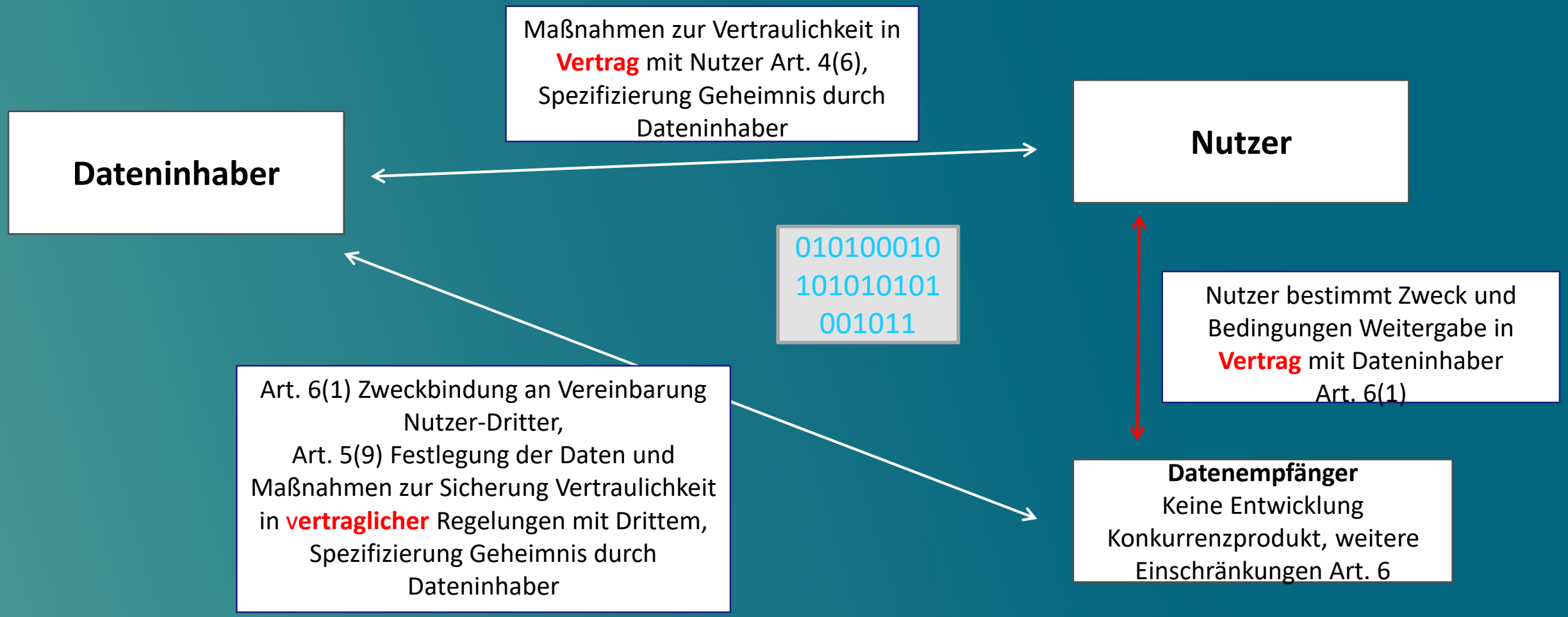
Keine abweichenden Vereinbarungen B2B, Art. 12 II DA

Missbrauchs- (AGB-)Kontrolle B2B, Art. 13 DA

"wenn Anwendung eine grobe Abweichung von der guten Geschäftspraxis bei Datenzugang und Datennutzung darstellt oder gegen das Gebot von Treu und Glauben verstößt"

Einschränkungen von Haftung, Gewährleistung, Nutzung

# Datenzugang und Geheimnisschutz



# Datenzugang und Geheimnisschutz im Konflikt

Assessment-Risiko – wie sicher feststellen, dass Geheimnis vorliegt und wer Inhaber ist?

- Geheimnisschutz von Rohdaten?
- Gefahr „überschießender“ Maßnahmen, wo kein Geheimnis vorliegt, insbesondere bei stärkerer Verhandlungsmacht

Vertrag Datenhalter - Nutzer Art. 4 – Offenlegung ggü. Nutzer

- Beschränkt freie Verfügung des Herstellers über n-pb Daten durch Notwendigkeit
- Vertrag mit Nutzer – Einschränkung Eigentumsrecht?
- „alle erforderlichen Maßnahmen“ zum Geheimnisschutz, Art. 4(6)
- Verweigerung der Datenweitergabe, Art. 4(7) bis (9)
  - Keine vertragliche Vereinbarung oder Verstoss gegen Geheimhaltung
  - Verweigerung bei Nachweis schweren wirtschaftlichen Schadens
  - Nutzer: Beschwerde bei Behörde, Streitbeilegungsstelle, Gericht

- Schutz von Geheimnissen auch bei Art. 3 DA?

# Datenzugang und Geheimnisschutz im Konflikt

- Art 5(9) Offenlegung gegenüber Dritten
  - Zweckbestimmung in Vertrag zwischen Nutzer und Drittem hinsichtlich Umfang
  - Offenlegung durch Datenhalter maßgeblich
  - Gefährdung des Schutzes für Dateninhaber durch weite Zweckbestimmung?
    - Relevanter „Zweck“? – beschränkt auf „aftermarket services“ für vernetzte Produkte oder auch Entwicklung ganz neuer innovativer Dienste durch Aggregierung, offen für Vermarktung auf Datenmärkten?
  - Vertrag zwischen Dateninhaber und Drittem
    - „unbedingt erforderliche“ Maßnahmen - Dritter verantwortlich
    - Schutz gegen Auferlegung übermäßig belastender Maßnahmen durch Dateninhaber aufgrund überlegener Verhandlungsmacht erforderlich – Art. 8, 13 ausreichend?
    - Sicherung Geheimnisschutz durch Vertragsketten bzw. § 4 Abs. 2 und 3 GeschGehG, insbes. auf Datenmärkten? Pflichten des unredlichen Empfängers, Art 11(2)DA

# Datenzugang und Datenschutzrecht im Konflikt

Bsp connected car – Maschinendaten und personenbezogene Daten untrennbar
Art. 1(5) Datenschutzrecht bleibt unberührt
Art. 4, 5 DA weiter als Art. 2 DSGVO (Datenportabilität)
DA keine Rechtsgrundlage im dsR Sinne
Nutzer: konkludente Einwilligung At. 6 I a DSGVO
Dritte:
- Art. 6 I b DSGVO
- Art. 6 I f DSGVO iVm Art. 6(2b) DA (Profiling)
- Art. 6 Ia, 7, 9 DSGVO - Einwilligung

Besondere Rolle Datenvermittlungsdienste (DGA)
PIMS
Anonymisierung

# Grenzüberschreitendes Datenrecht – Anwendungsbereich DA und IPR

## Art. 1(3) DA

- Hersteller und Anbieter von Produkten und zusammenhängenden Dienstleistungen, die in der EU angeboten werden sowie die damit zusammenhängende Nutzung in der EU
- Dateninhaber, die Daten an Dritte in der EU zugänglich machen
- Datenempfänger in EU, denen Daten zugänglich gemacht werden
- Datenverarbeitungsdienste, die an Kunden in der EU angeboten werden
- Keine IPR-Regeln

## IPR und Opt-Out

Charakter der Zugangsrechte – Lauterkeitsrecht = Art. 1(3) DA
Vertragsrecht = ROM I
Auch bei zwingendem Recht vertragliches Opt-Out möglich, Art. 3(1) ROM-I, anders bei Verbrauchern, Art. 6(4)
Art. 3(4) ROM I – kein opt-out bei reinen Binnensachverhalten – Auslandsbezug vorhanden`?

# Besondere Regeln Drittstaatentransfer nicht-pb. Daten

## Ch. VI – Cloud-Switching Art. 23 ff.

Diensteanbieter muss hohes Sicherheitsniveau beim „Switching“ anbieten
Detaillierte Vorgaben für Vertrag
Art. 29 – Information auf Website über technische, organisatorische und vertragliche Maßnahmen zum Schutz gegen internationalen Regierungszugriff, der nicht im Einklang mit europäischem oder nationalen Recht

## Ch. VII - Transfer und Zugang für Behörden aus Drittstaaten Art. 32

Diensteanbieter müssen technische, organisatorische und vertragliche Maßnahmen zum Schutz gegen internationalen Regierungszugriff auf nicht-personenbezogene Daten treffen, der nicht im Einklang mit europäischem oder nationalen Recht
Bedingungen für Compliance mit drittstaatlichem Urteil oder Verwaltungsentscheidung zum Datenzugang

# Zwischenfazit

**(+)**

- Regeln Cloud Switching
- Förderung Interoperabilität
- AGB -Kontrolle B2B

**(-)**

- Zugang zu Rohdaten meist nicht ausreichend, Ausschluss aggregierte Daten (KI)
- Öffnung für Sekundärmärkte möglich?
- FRAND unklar
- Kohärenz, Schnittstellen zu Geheimnisschutz und Datenschutzrecht
- (grundstzliche) Probleme des nutzerzentrierten Modells
  - Rollenverteilung unterkomplex
  - Transaktionskosten und  Informationsasymmetrien
  - Faktische und vertragliche Stellung Dateninhaber/Hersteller bleibt stark
  - Rolle für Datenintermediäre, Art. 9 ff. DGA
  - Business Monitoring nicht ausgeschlossen
- Welches Marktversagen regelt Data Act?

**Data Act nur als Basisregulierung (?)**

Data Spaces

Sektorspezifische Regulierung

# Innovation am Bsp. Connected cars

Marktversagen

- Wirklich zu wenig Daten bereitgestellt?
- Kontrolle des Zugangs zu Daten und Funktionen des Fahrzeugs („in-vehicle data and resources“) schließt Wettbewerb unabhängiger Diensteanbieter auf den Märkten für nachgelagerte und komplementäre Dienste aus
- Strategien: Zugangskontrolle, vertragliche Koppelung der Dienste
- Ergebnis: Diskriminierung, Monopolpreise, völliger Ausschluss des Zugangs
- zu geringes Maß an Interoperabilität und Offenheit des Ökosystems bedingt weniger Verbraucherauswahl, Unternutzung der Daten und weniger Innovation

Wichtige Leitprinzipien

- fairer und nicht-diskriminierender Wettbewerb
- Interoperabilität zwischen Anwendungen durch standardisierten Zugang

# Sektorspezifische Zugangsregelungen am Bsp. Kfz-Bereich

- **Kfz-GVO 461/2010**
  - Art. 61: Zugang zu Reparatur- und Wartungsinformation
  - Direkte Zugangsrechte für dritte Unternehmen und autorisierte Betriebe
  - Bereitstellung von Informationen über das Internet,
  - Weiterverwendung aufgrund Vertrag mit Hersteller, Zi. 6.1. Anl. X

- **Vorschläge EU zur Überarbeitung TypGVO 2018/858**
  - Zugang zu Funktionen und HMI (Kommunikation mit Fahrer) sowie Fernzugriff
  - Vorgabe Grundbestand von Daten und Formaten
  - Einbeziehung öffentlicher Interessen (Umweltschutz, Verkehrssicherheit)

-

# Weitergehende Regulierungsoptionen – Datenzugang Connected car

- **Extended vehicle-Konzept**
  - Bereitstellung Daten über Webschnittstelle, kein direkter Zugriff
  - Hersteller hat Zugangskontrolle
  - Angebote von Datenpaketen, BMWCarData, Caruso (Mercedes-Benz)
  - Erweiterung ADAXO: Zugriff auf Daten im Auto über Schnittstelle, alle Daten und Funktionen, die für eigene Dienste genutzt, Zugriff zu FRAND-Bedingungen
  - Hersteller bleiben Gatekeeper, vertragliche Regelungen
- **Data Shared Services**
  - Daten auf unabhängig betriebener Plattform
  - Einbindung eines Datentreuhänders, "Mobilitätsdatenwächter"
  - Kein direkter Datenzugang der Marktakteure per Fernzugriff auf Fahrzeugdaten sowie -funktionen und -ressourcen
- **OTP**
  - Offene und interoperable Telematik-Plattform, ins Kfz integriert,
  - direkter, standardisierter, diskriminierungsfreier Zugang zu den Daten im Fahrzeug .
  - Herausforderung für die OTP: IT-Sicherheit des Zugangs über das gesamte Fahrzeugleben gewährleisten.

# Regulierungsoptionen

## Langfristig: OTP-Modell

- Direkter und gleichberechtigter Zugriff auf Daten, Funktionen und HMI (API)
- Funktionstrennung „eingebaut" – vernetztes Fahrzeug als offenes System
- Weitgehende Anforderungen an Standardisierung, Kompatibilität und IT-Sicherheit

→ Regulatorische Aufgabe

- Klar geregeltes Zugangs- und Berechtigungskonzept für Daten, Funktionen und Ressourcen
  - Weitgehende Entscheidungsfreiheit beim Nutzer
  - Einbeziehung öffentlicher Interessen durch Datentreuhand, die in Datenmanagement einbezogen wird
- Aufsetzen auf Änderungsvorschlag TypGVO oder Data Act
- Langfristig beste Lösung für Förderung von Wettbewerb und Innovation

# Fazit

- Immaterialgüterrechte an Daten nicht möglich und wünschenswert
- Data Governance: Faktische Kontrolle, Vertragsrecht und Zugangsrechte
- Datenvertragsrecht ist in der Entwicklung
- Data Act schafft Basis für Zugangsrechte
- Defizite: Beschränkung auf Rohdaten, nutzerzentriertes Modell
- Ergänzung durch sektorspezifische Regulierung notwendig
- Wichtige Rolle von Intermediären/Datentreuhand
- Datensicherheit, Standardisierung und Kompatibilität fördern
- Innovation kann weitergehende Regulierung für Herstellung „level-playing-field" erfordern

# Literaturhinweise


- Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4136484
- Kerber, Wolfgang: Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data, Jipitec 2018, 310
- Kerber, Wolfgang: Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives (GRUR Int. 2022, 107
- Leistner/Antoine, IPR and the use of open data and data sharing initiatives by public and private actors, Study requested by the JURI committee of the European Parliament, 2022, https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)732266
- Metzger/ Schweitzer, Shaping Markets: A Critical Evaluation of the Draft Data Act, ZEuP 2023, 82
- Wiebe, The Data Act Proposal – Access rights at the Intersection with Database Rights and Trade Secret Protection, GRUR Int. 2023, 227
- Wiebe, Der Data Act - Innovation oder Illusion?, GRUR 2023, 1569
- Wiebe, Der Data Act als vertragsrechtlicher Rahmen für Datennutzungsverträge unter besonderer Berücksichtigung der Missbrauchskontrolle von Art. 13 DA, CR 2023, 777

# Danke für die Aufmerksamkeit!

Andreas.Wiebe@jura.uni-goettingen.de