GRUR-Jahrestagung 2022

Fachausschuss Recht der Daten

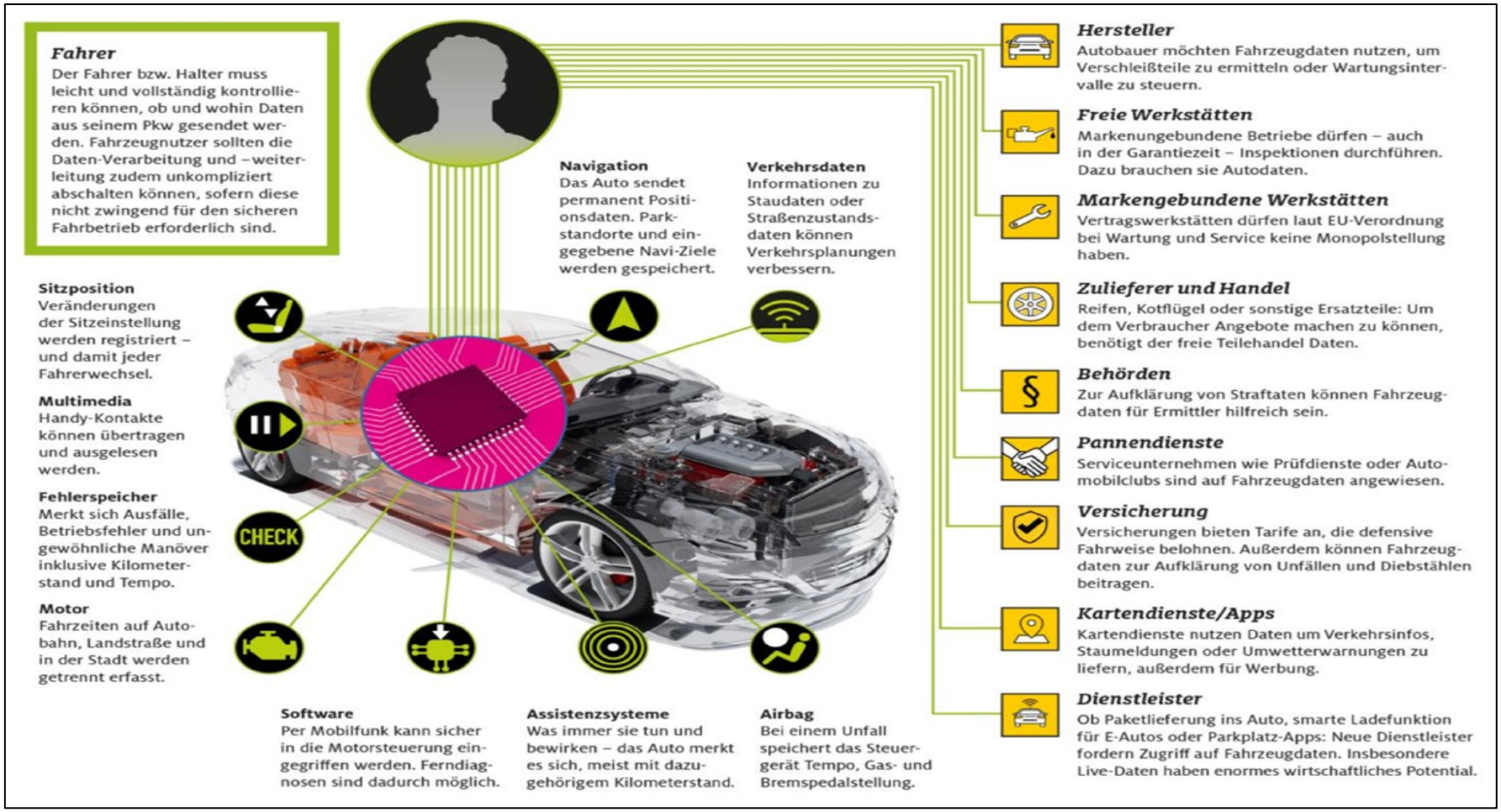
Verhältnis von Data Act und Datenbankherstellerrecht bzw. Geheimnisschutz

6.10.2022

Prof. Dr. Andreas Wiebe, LL.M. ((Virginia)

Professur für Bürgerliches Recht, Wettbewerbs- und Immaterialgüterrecht, Medien- und Informatinosrecht, Georg-August-Universität Göttingen

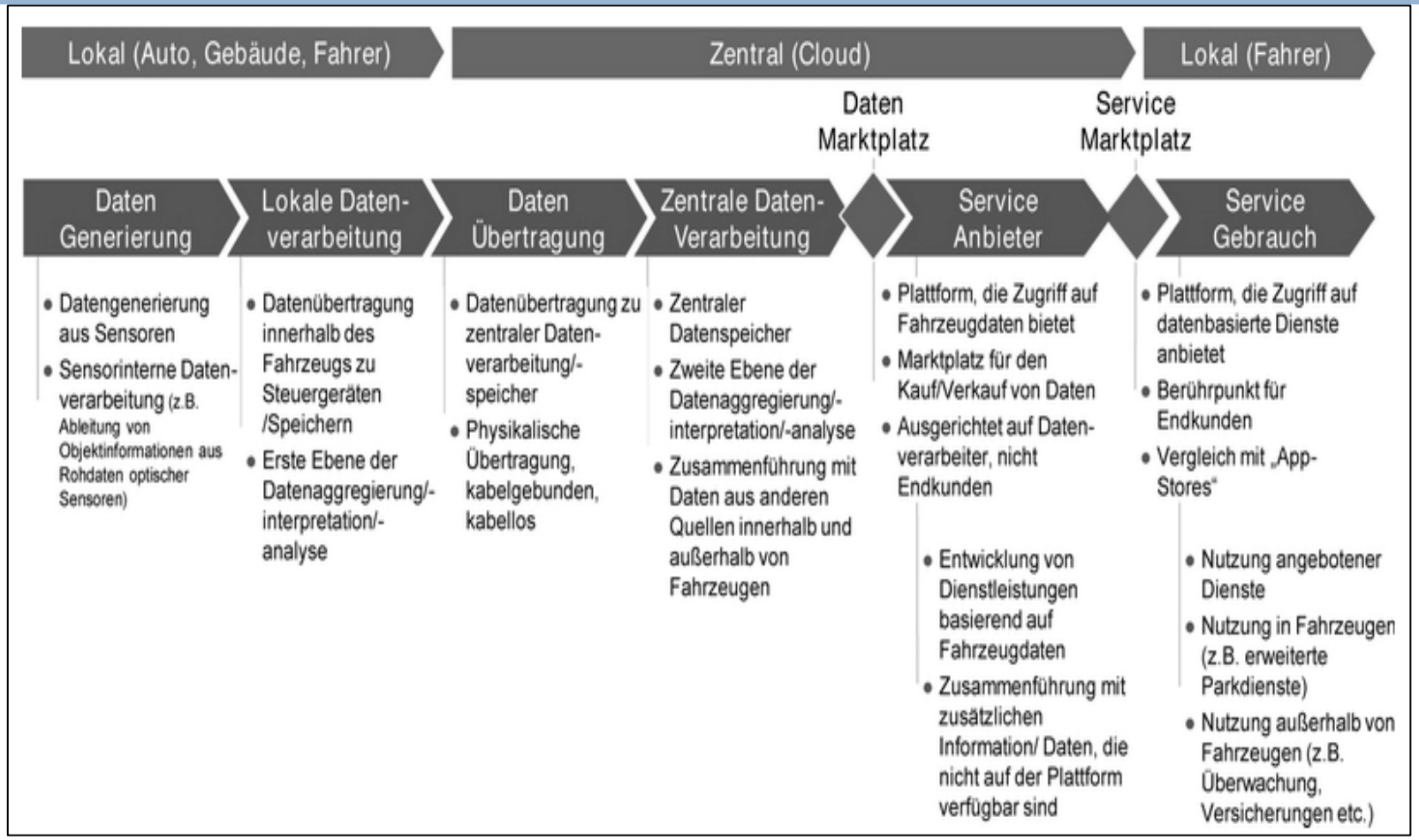
Beispiel „connected car“



Datenerzeugung

ADAC Motorwelt

Beispiel „connected car“



Wertschöpfungskette

Burkard/Koehler/König/Olschewski, Monetizing Automotive Data, S. 9

Datenbankherstellerrecht §§ 87a ff. UrhG

- "Outdated legal framework" (2018 Evaluation) ?
  - In der Praxis noch nicht stark genutzt, aber mit enormem Potenzial in der Datenwirtschaft
- Ist das Datenbankherstellerrecht hinderlich für Zugang und Nutzung von Daten?
  - Faktische Kontrolle plus rechtlichem Schutz von Datenbanken
  - Gefahr der Behinderung der Aggregierung von Rohdaten und Schaffung von Mehrwert mit der Folge eines Marktversagens
- Relevante tatsächliche Fragen:
  - Wann werden welche Daten aus geschützten Datenbanken entnommen?
  - Sind Rohdaten bzw. maschinengenerierte Daten (MGD) vom Schutz umfasst?
  - Wie sind die Auswirkungen auf die Nutzung von KI unter Einsatz von Trainingsdaten?

Einbeziehung von Maschinendaten ?

- Einerseits: geringe (Schutz-)Anforderungen an Investitionen
  - Aber: Investitionsanreize nicht erforderlich
- Andererseits Unsicherheit über Erfassung von MGD
  - EuGH 2004: Unterscheidung Generierung / Sammlung von Daten, Investitionen in Sammlung müssen separat nachgewiesen werden, kaum Schutz für by-products
  - Unterschiedliche Rechtsprechung, z.B., BGH, GRUR 2010, 1004 – Autobahnmaut: Registrierung von LKW-Daten an Terminals von Toll Collect als Sammlung → anknüpfende Dienste erschwert
  - *Leistner*: per Sensoren erhobene Daten können von jedem Dritten erhoben werden = Sammlung
  - Traktor erhebt Daten über Zustand des Ackers = Sammlung oder Generierung?

→ *Rechtsunsicherheit*

Einbeziehung von MGD ?

- Praktische Abgrenzungsprobleme
  - Beispiel: Daten, produziert durch Maschine in Produktionslinie, werden zunächst kategorisiert und dann automatisch und methodisch durch Industrieroboter arrangiert
  - Die unmittelbar folgenden technischen Prozesse ("data curation") sind untrennbar mit dem Generierungsprozess verknüpft und erfolgen vor der Speicherung ("real-time processing")

  -> Abgrenzung Generierung / Sammlung praktisch nicht durchführbar
  - Auf spezifische Datenbank gerichtet?
- Probleme der Zuordnung und Co-ownership
  - Welche Datenbank ist Ziel und wer ist "Hersteller"?
- Möglicher Schutz für sole-source-Datenbanken

-> Ausschluss von MGD aus Datenbankherstellerrecht

Wie Ausschluss umsetzen?

- Explizite Ausschlussklausel für MGD

  Begleitstudie zum Datenbankrecht:

  - *MGD is defined as data recorded, collected, or generated independent of direct and economically significant human intervention by:*
    - *computer processes, applications or services.*
    - *sensors processing information received from equipment, software or machinery, …*
      - data generated by sensors about the sensor and machine itself, e.g. data on machine performance;
      - data generated/observed by sensors observing the environment in which sensors and machines operate, e.g. information on the soil recorded by sensors in smart tractors;
      - data resulted from the aggregations and processing of the two types of data above.

- Konkretisierung der Anforderungen an Wesentlichkeit der Investition

  Minimum level, begünstigt große Datenbanken = MGD Datenbanken

  Vorschlag: Durchschnittsinvestition per Dateneinheit, MGD günstig erlangt, große Datenbanken

Data Act Proposal (Vorschlag für ein Datengesetz)

Artikel 35

Datenbanken, die bestimmte Daten enthalten

- Damit die Ausübung des Rechts der Nutzer auf Zugang zu solchen Daten und deren Nutzung nach Artikel 4 dieser Verordnung oder des Rechts auf Weitergabe solcher Daten an Dritte nach Artikel 5 dieser Verordnung nicht behindert wird, findet das in Artikel 7 der Richtlinie 96/9/EG festgelegte spezifische Schutzrecht sui generis keine Anwendung auf Datenbanken, die Daten enthalten, die bei der Nutzung eines Produkts oder verbundenen Dienstes erlangt oder erzeugt wurden.

- Interpretation ?
  - Klarstellung, dass die Schutzanforderungen nicht erfüllt sind (Erwgrd. 84)
  - Gesetzliche Ausnahme vom Anwendungsbereich der DatenbankRL
  - Beschränkung der Verwertungsrechte im Umfang der Zugangsrechte nach Art. 4 und 5 des DA-E

-> klarstellen

Art. 35 – Probleme

- Anwendung auf “mixed databases”?
  - Praxis “connected car”: in-vehicle access -> MGD, “off-vehicle” -> Mix und Aggregierung von MGD und anderen Datenarten
  - Wortlaut scheint alle Datenbanken zu erfassen, die MGD enthalten
    - Bereits ein Datensatz ausreichend?
    - Wie lassen sich MGD erfassen und abtrennen ?
  - Praktikable Ausschlussklausel?
    - ~ Leitlinien freier Verkehr nichtpersonenbezogener Daten (2019):

      MGD und andere Daten “untrennbar miteinander verbunden”

      –> Datenbankschutz ausgeschlossen, +
    - Durch Hersteller widerlegliche Vermutung, dass mixed databases vom Schutz ausgeschlossen

Art. 35 – Defizite

- Anwendungsbereich
  - Art. 1(1) DA-E – auf bei Nutzung von IoT generierte oder erlangte Daten beschränkt – nicht alle MGD erfasst
    - Fahrzeug als Ganzes erfasst oder nur hinsichtlich einzelner Funktionsbereiche?
    - Klarstelllung, dass data curation nicht aus Anwendungsbereich herausführt
  - Aggregierte/abgeleitete Daten nicht erfasst
      - Erwgrd. 14: gleichzeitig sollten aus diesen Daten abgeleitete oder gefolgerte Informationen, sofern sie rechtmäßig erlangt wurden, nicht in den Anwendungsbereich dieser Verordnung fallen.
      - Erwgrd. 17: "jedoch nicht Daten, die sich aus einem Softwareprozess ergeben, mit dem abgeleitete Daten aus solchen Daten berechnet werden…"
    - Praktische Abgrenzung der ausgeschlossenen Daten kann in vernetzter Umgebung schwierig sein und zu einem Schutz von MGD führen
    - Datenbankrecht greift ein - Data sharing hinsichtlich abgeleiteter und aggregierter Daten kann gerade für innovative Dienste notwendig sein

-> Erweiterung des Ausschlusses auf aggregierte Daten

Weiterer Änderungsbedarf Datenbankrecht

- Weitere Vorschläge für Änderungen der DatenbankRL
  - Anpassung an generelle Urheberrechtsschranken
  - Einführung spezifischer Schranken, z.B. für web scraping, Suchmaschinen
  - Schranken Art. 6, 9 DatenbankRL zwingend gestalten und die Nutzung ganzer Datenbanken für Forschungszwecke zulassen
  - Einführung von Zwangslizenzen für sole-source Datenbanken
    - Möglich auch im Rahmen sektorspezifischer Regelungen
  - Ausnahme vom Datenbankherstellerrecht für öffentliche Einrichtungen
  - Verkürzung der Schutzdauer

Weiterer Änderungsbedarf Datenbankrecht

- EuGH, C-762/19, GRUR 2021, 1075 - *CV-Online v Melons*
- Flexibler lauterkeitsrechtlicher Test (Leistungsübernahme) hinsichtlich Beeinträchtigung der Amortisation der Datenbankinvestition
  - Bedürfnis für weitere Schranken obsolet?
  - Anwendung und zukünftige Entwicklung unsicher
  - Spricht dies für erneute Einbeziehung von MGD in Datenbankherstellerrecht?
  - Aggregierte data sets (big data, AI training) sind wahrscheinlich auch unter *CV Melons* geschützt

  -> potentielle Beeinträchtigung des Data sharing bleibt

  -> Ausweitung von Art. 35 auf MGD einschl. aggregierter und abgeleiteter Daten, oder

  -> Zwangslizenzierung von aggregierten Data sets

Geheimnisschutz (GeschGehG) und Daten

- Geheimnisschutz von Rohdaten/MGD?
- § 2 Nr. 1: „*Geschäftsgeheimnis (ist) eine Information…*“
  - Geschützt sind Informationen (semantische Ebene), nicht Daten (syntaktische Ebene/digitale Kodierung)
  - Information, die in Datensatz enthalten
  - Schutz wird für einzelnes Datum und/oder Rohdaten/MGD abgelehnt
  - Technische Bearbeitung, Auswahl, Aggregierung von Datensätzen – Schaffung von Bedeutung und Wert
  - → lässt sich Rohdaten/MGD bereits Bedeutung entnehmen?
  - Zumindest nach (teilweise untrennbar verbundener) technischer Bearbeitung

Geheimnisschutz und Daten

- *„…a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile…bekannt oder ohne Weiteres zugänglich ist…“*
- *„…und daher von wirtschaftlichem Wert ist“*
  - Verbesserung der Wettbewerbslage des Unternehmens
  - Kausalität zwischen Geheimsein und wirtschaftlichem Wert
  - Von IoT Produkt generierter Datensatz ausreichend werthaltig?
    - Einzelfallfrage, potenzieller Wert ausreichend
    - Wert nicht durch Nützlichkeit sondern Geheimhaltung
    - Bsp. Technische Information als Grundlage für Wartung (Drexl 2018)
  - Aggregierung und Kombination mit anderen Daten generiert Wert, etwa zu Zwecken der Weiterentwicklung von Produkten

Geheimnisschutz und Daten

- *„b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist“*
  - Herausforderung durch horizontale und vertikale Integration, Sharing-Plattformen
    - Verstärkte organisatorische, technische, rechtliche Maßnahmen
  - Auswirkungen von Data analytics:
    - Erlangung von Geheimnissen durch Dritte mittels Big Data-Analyse als gegen Treu und Glauben und anständige Marktgepflogenheiten (§ 4 Abs. 1 Nr. 2 GeschGehG)
    - Data analytics und reverse engineering (§ 3 Abs. 1 Nr. 2 GeschGehG)
      - Spezifische Geheimhaltungsklauseln gegen Reverse Engineering bei vertraglicher Überlassung möglich (Nr. 2 b), soweit nach allgemeinen Grundsätzen rechtmäßig (AGB, Kartellrecht), wohl nicht bei Kaufverträgen
      - Umgehung technischer Schutzmaßnahmen
  - Perspektive: Verschlüsselungstechniken
    - Homomorphic cryptography – Verarbeitung ohne Zugang zum Inhalt
    - Secure Multiparty Computation (SMC) – nur eigener Input zugänglich

Geheimnisschutz und Daten

- Inhaber/Rechtezuordnung - „*Rechtmäßige Kontrolle*“ (§ 2 Nr. 2 GeschGehG)
  - Wirtschaftliches Interesse und Organisationshoheit über Daten - Hersteller
  - Smart Factory – Geheimnisse des Unternehmens verarbeitet (Nutzer)
  - Smart Car: nicht Eigentümer, sondern Hersteller des Datenerhebungsgeräts oder dritter Dienstleister
  - Vernetzte Systeme/Cloud Services – Vielzahl von Ko-Inhabern oder Verlust der Kontrolle?

- Schutzumfang § 4 GeschGehG

  → Kontrolle der Nutzung und Weitergabe durch Datennutzungsverträge mit entsprechenden Beschränkungen

Geheimnisschutz und Data Act

- Know-how-transfer im Rahmen in der eigenen Produktionskette
  - Bilaterale und unilaterale Verträge, Data Sharing als Erweiterung
  - Bereitschaft zum Data Sharing (auch) abhängig von effektivem Geheimnisschutz
- Konflikt mit Data Act ?
  - Ausschluss von MGD im Interesse des data sharing?
  - Konfliktbereich bei Rohdaten praktisch eher klein (s.o.),
    - anders bei vorgeschlagener Erweiterung auf aggregierte und abgeleitete Daten
- Koexistenz ohne besondere Regelung?
  - Art. 3(2) GehRL: Erwerb, Nutzung oder Offenlegung eines Geschäftsgeheimnisses als rechtmäßig, als...durch Unionsrecht oder nationales Recht vorgeschrieben oder erlaubt.
    - Data Act erlaubt Zugang und Nutzung
  - Art. 5(d) GehRL: Ausnahme bei Nutzung oder Offenlegung "zum Schutz eines durch das Unionsrecht oder das nationale Recht anerkannten legitimen Interesses"
    - Data Act dient Interesse an Innovationsförderung durch data sharing

Data Act Proposal

- Art. 4 (Dateninhaber – Nutzer)
- (3) Geschäftsgeheimnisse werden nur offengelegt, wenn alle besonderen Maßnahmen getroffen worden sind, die erforderlich sind, um die Vertraulichkeit der Geschäftsgeheimnisse, insbesondere gegenüber Dritten, zu wahren. Der Dateninhaber und der Nutzer können Maßnahmen vereinbaren, um die Vertraulichkeit der gemeinsam genutzten Daten, insbesondere gegenüber Dritten, zu wahren.
- (4) Der Nutzer darf die aufgrund eines Verlangens nach Absatz 1 erlangten Daten nicht zur Entwicklung eines Produktes nutzen, das mit dem Produkt, von dem die Daten stammen, im Wettbewerb steht.
- Art. 5(8) (Nutzer - Dateninhaber – Dritter)

  Geschäftsgeheimnisse werden Dritten gegenüber nur insoweit offengelegt, als dies für den zwischen dem Nutzer und dem Dritten vereinbarten Zweck unbedingt erforderlich ist und der Dritte alle zwischen ihm und dem Dateninhaber vereinbarten besonderen Maßnahmen getroffen hat, die erforderlich sind, um die Vertraulichkeit des Geschäftsgeheimnisses zu wahren. In diesem Fall werden die Eigenschaft der Daten als Geschäftsgeheimnisse und die Maßnahmen zur Wahrung der Vertraulichkeit in der Vereinbarung zwischen dem Dateninhaber und dem Dritten festgelegt.

Data Act Proposal – Praktische Probleme von Information und Kontrolle

- Assessment-Risiko – wie kann man sicher feststellen, dass Geheimnis vorliegt und wer Inhaber ist?
  - Durch digitale Umgebung erschwert
  - Unsicherheit über Bestehen Geheimnis kann zu "überschießender" Geltendmachung trotz fehlendem Schutz (overclaiming") führen – Beeinträchtigung des data sharing
- Vertrag Datenhalter - Nutzer Art. 4 – Offenlegung ggü. Nutzer
  - Beschränkt freie Verfügung des Herstellers über n-pb Daten
    - zB Hersteller von Komponenten bei „connected cars"
  - „besondere", „erforderliche Maßnahmen" zum Geh.schutz ?
  - Vertragliche Regelung – Missbrauchsrisiko zu Lasten Nutzer?
  - Modellverträge, einschl. technischer und organisatorischer Maßnahmen
  - Verschlüsselung, sichere Verarbeitungsumgebungen (Art. 5(3) Data Governance Act Proposal 2020, version EP 6.4.2022)
  - Generelles Problem: Rollenzuordnung Datenhalter/Nutzer in komplexen Wertschöpfungsketten

Data Act Proposal - Praktische Probleme von Information und Kontrolle

- Art 5(8) Offenlegung gegenüber Dritten
  - Zweckbestimmung in Vertrag zwischen Nutzer und Drittem hinsichtlich Umfang Offenlegung durch Datenhalter maßgeblich
  - Gefährdung der Schutzes für Datenhalter durch weite Zweckbestimmung?
    - Relevanter „Zweck“? – beschränkt auf „aftermarket services“ für vernetzte Produkte oder auch Entwicklung ganz neuer innovativer Dienste (Erwgrd. 28), auch Aggregierung, offen für Vermarktung auf Datenmörkten? – klarstellen!
    - Art. 6(2)(e) – Ausschluss der Entwicklung von Konkurrenzprodukt durch Dritten
  - Vertrag zwischen Dateninhaber und Drittem
    - „unbedingt erforderliche“ Maßnahmen - Dritter verantwortlich
    - Schutz gegen Auferlegung übermäßig belastender Maßnahmen durch Datenhalter 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-E
    - Wie kann Nutzer als Geheimnisinhaber Schutz gegen Dritten sicherstellen?

Data Act Proposal und Geheimnisschutz - Zwischenbilanz

- Einschränkung Geheimnisschutz durch Zugangsrechte erscheint gerechtfertigt
- Klausel zum Ausschluss von Geheimnisschutz bei MGD (~ Art. 35) würde Geheimnisschutz zu stark einschränken und data sharing beeinträchtigen
- Praktische Unsicherheit bei Voraussetzungen Geheimnisschutz allgemein → Guidelines, Musterverträge
- Unklarheit, welche Daten erfasst, setzt sich in der Wertschöpfungskette fort und schafft Unsicherheiten für Dritte hinsichtlich GeschGehG-Verletzung
  - Notwendigkeit klarer vertraglicher Regelungen (etwa Art. 5(8))
  - Schutz gegen missbräuchliche Gestaltung (Art. 13, AGB-Recht, Kartellrecht)
- Einsatz technischer Schutzmöglichkeiten für Geheimnisschutz hohe Relevanz
  - Art. 11 (einschl. smart contracts) als ausreichender Schutz gegen Missbrauch durch Dateninhaber, oder (umgekehrt) zu starke Beschränkung des Zugangs?
  - „in-situ-access“ – geringere Gefährdung von Geheimnissen durch Verschaffung von Zugang für Nutzer und Dritte durch Dateninhaber

Zusammenfassung

- Grundsätzlich Zugangsrechte und IP/Geh.schutz kompatibel, aber rechtliche Schärfung der Schnittstellen und praktische Effektivierung notwendig
- Begrenzter Anwendungsbereich DA-E, insbes. hinsichtlich aggregierter Daten kann die positiven Effekte des Ausschlusses von MGD vom Datenbankrecht und der Regelungen zur Nutzung von Geheimnissen beeinträchtigen
- Ausschluss von MGD vom Datenbankherstellerrecht sollte auf aggregierte/abgeleitete Daten ausgeweitet und konkretisiert werden
- Es bedarf einer konkretisierenden Regelung für Erfassung von mixed databases
- Weitere Reform des Datenbankherstellerrechts bleibt auf der Tagesordnung, relativiert durch die neuere Rechtsprechung des EuGH (*CV Melons*)

Zusammenfassung

- Probleme der Feststellung von Schutzgegenstand und Schutzumfang beim Geheimnisschutz werden durch digitale Datenwirtschaft verstärkt
- Zugangsrechte schaffen Informations- und Kontrollprobleme im Dreiecksverhältnis Dateninhaber – Nutzer - Dritter
- Der Data Act-E schafft keine neuen Regelungen zum Geh.schutz, sondern betont zutreffend die Bedeutung vertraglicher Regelungen, die durch Guidelines und Musterverträge zu fördern sind
- Technische Schutzmaßnahmen haben große Bedeutung für Geheimnisschutz
- Weitere Ergänzungen sektorspezifisch sinnvoll
- Funktionsfähigkeit des nutzerzentrierten Vermarktungsmodells muss sich in Praxis bewähren

Begleitstudien zum Thema

- STUDY TO SUPPORT AN IMPACT ASSESSMENT FOR THE REVIEW OF THE DATABASE DIRECTIVE, Final Report, 2022, https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act
- STUDY ON THE LEGAL PROTECTION OF TRADE SECRETS IN THE CONTEXT OF THE DATA ECONOMY (GRO/SME/20/F/206) FINAL REPORT, July 2022, https://op.europa.eu/en/publication-detail/-/publication/c0335fd8-33db-11ed-8b77-01aa75ed71a1/language-en
- Drexl, Data Access and Control in the Era of Connected Devices Study on Behalf of the European Consumer Organisation BEUC, 2018, https://www.beuc.eu/sites/default/files/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf
- Drexl u.a., 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), Research Paper No. 22-05
- 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 EP, 2022

Herzlichen Dank !

andreas.wiebe@jura.uni-goettingen.de