Deutsche Stiftung für Recht und Informatik

SCHUTZ VON GESCHÄFTSGEHEIMNISSEN IM SPANNUNGSVERHÄLTNIS ZUM DATA ACT

Dr. Jonathan Kropp

Dr. Julia Freifrau von Imhoff

Taylor Wessing PartG mbB

Herbstakademie 2024

Referenten

Dr. Jonathan Kropp

Rechtsanwalt, München
+49 89 21038-0
J.Kropp@taylorwessing.com

Jonathan Kropp ist auf die Beratung im IT-, Urheber- und Medienrecht spezialisiert.

Einen Schwerpunkt seiner Tätigkeit bildet dabei die Vertretung von Unternehmen bei gerichtlichen und außergerichtlichen Streitigkeiten im Technologie-Bereich, insbesondere bei Softwarestreitigkeiten sowie gescheiterten IT-Projekten.

Dr. Julia Freifrau von Imhoff

Rechtsanwältin, München
+49 89 21038-0
J.Imhoff@taylorwessing.com

Julia von Imhoff ist Mitglied der Practice Area Technologie, Medien & Telekommunikation (TMT).

Schwerpunktmäßig berät Julia Freifrau von Imhoff insbesondere im Bereich Tech Litigation zu IP/IT-rechtlichen Fragestellungen, Geschäftsgeheimnisverletzungen sowie urheber- und wettbewerbsrechtlichen Streitigkeiten.

Agenda

1 Einführung

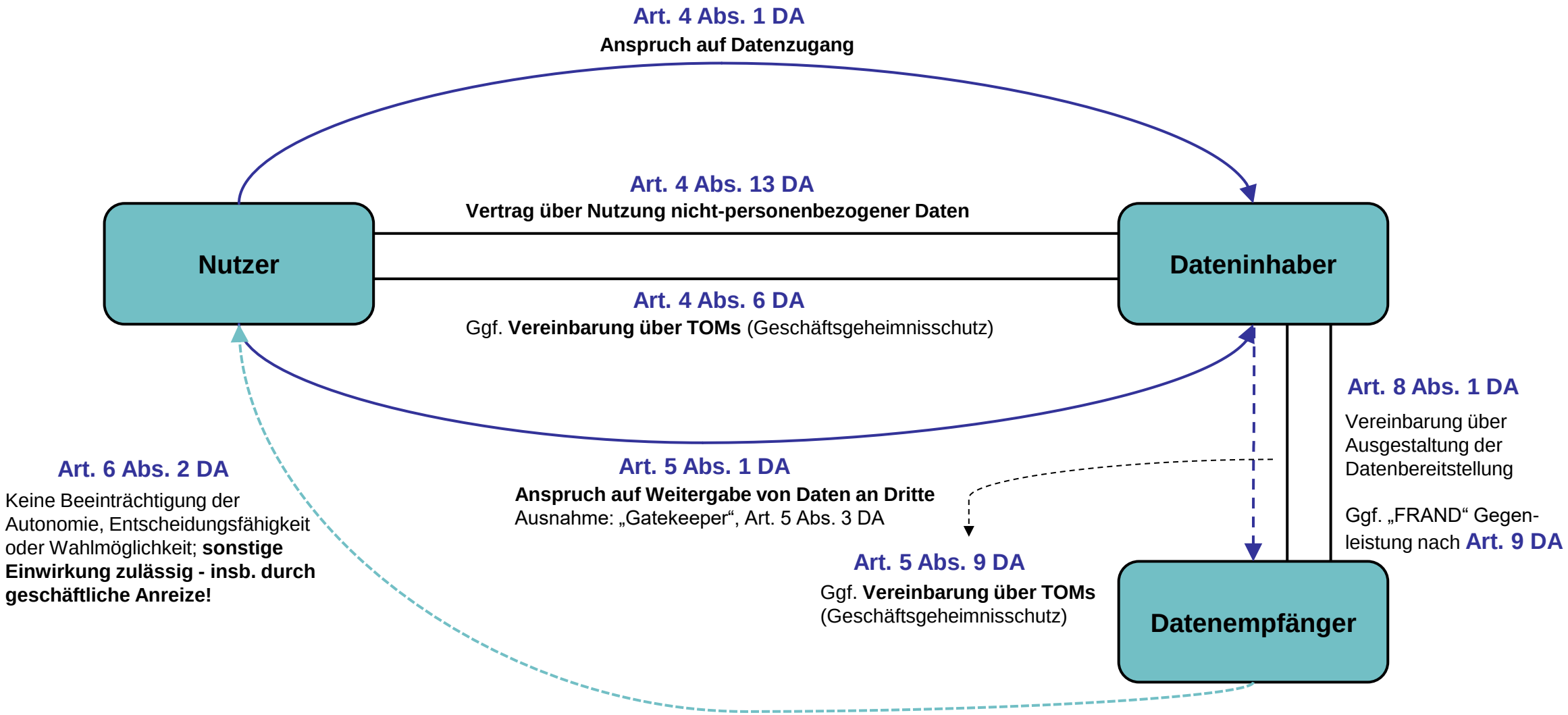
2 Schutz von Geschäftsgeheimnissen
Verhältnis Nutzer / Dateninhaber

3 Schutz von Geschäftsgeheimnissen
Verhältnis Datenempfänger / Dateninhaber

4 Umsetzung des DA

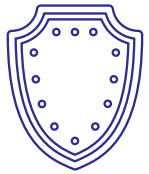
(1) Einführung

Datenzugang nach dem Data Act



(2) Schutz von Geschäftsgeheimnissen im Verhältnis Nutzer vs. Dateninhaber

„Primärer“ Schutz von Geschäftsgeheimnissen, Art. 4 Abs. 6, 7, 8 DA



- Offenlegung (und Nutzung) von Geschäftsgeheimnissen im Verhältnis Dateninhaber und Nutzer grundsätzlich vorgesehen (ErwG 31)
- **Schutz:** Durch Vereinbarung von angemessenen technischen und organisatorischen Maßnahmen (TOMs) zwischen Dateninhaber und Nutzer, insbesondere um Vertraulichkeit gegenüber Dritten zu wahren (Abs. 6).
  - ❖ Mustervertragsklauseln, Vertraulichkeitsvereinbarungen (NDAs), strenge Zugangskontrollen, technische Normen, Anwendung von Verhaltenskodizes
- **Verweigerungsrecht:** Wenn keine Einigung über TOMs oder vereinbarte TOMs vom Nutzer nicht umgesetzt werden oder Vertraulichkeit der Geschäftsgeheimnisse vom Nutzer verletzt wird (Abs. 7).
- **Verweigerungsrecht „unter außergewöhnlichen Umständen“**: Wenn trotz getroffener TOMs der Dateninhaber „mit hoher Wahrscheinlichkeit“ einen „schweren wirtschaftlichen Schaden“ erleidet (Abs. 8).
  - ❖ Hierfür jeweils notwendig: Begründung und Mitteilung an zuständige Aufsichtsbehörde, im Falle von Abs. 8 auf der „Grundlage objektiver Fakten“ (z.B. Durchsetzbarkeit des Geheimnisschutzes in Drittländern).

„Flankierender“ Schutz durch Nutzungsverbote, Art. 4 Abs. 10 DA

Nutzungsverbote

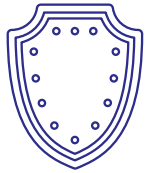
…verhindern nicht den Zugang, sollen aber bestimmte „unerwünschte“ Nutzungsmöglichkeiten unterbinden:

1. Keine Nutzung zur Entwicklung eines IoT-Produkts, das mit dem vernetzten Produkt im Wettbewerb steht (oder Weitergabe an Dritte zu diesem Zweck), Art. 4 Abs. 10 Alt. 1 DA.
2. Keine Nutzung um Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden des Herstellers / Dateninhabers zu erlangen, Art. 4 Abs. 10 Alt. 2 DA.

„Flankierender“ Schutz durch technische Schutzmaßnahmen, Art. 11 Abs. 1 DA

Technische Schutzmaßnahmen

Der Dateninhaber kann nach Artikel 11 Abs. 1 DA technische Schutzmaßnahmen implementieren, um:



1. die Einhaltung der Artikel 4, 5, 6, 8 und 9 DA sicherzustellen, und
2. einen unbefugten Datenzugang zu verhindern.

Beachte: Anders als in der englischen Fassung von Artikel 11 DA fehlt der Verweis auf Artikel 4 DA in der deutschen Fassung. Das dürfte ein redaktionelles Versehen sein.

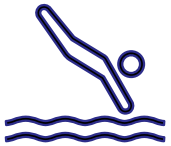
Weitere Abwehrmöglichkeiten des Dateninhabers

…durch vertragliche Beschränkungen, Art. 4 Abs. 2 DA

- Nur in engen Ausnahmefällen, wenn die Sicherheitsanforderungen des IoT-Produkts durch Zugang, Nutzung oder Weitergabe der Daten beeinträchtigt werden und dies zu schwerwiegenden nachteiligen Auswirkungen auf die Gesundheit oder Sicherheit von natürlichen Personen führen könnte.
- Erforderlich: Mitteilung an zuständige Aufsichtsbehörde.

Weitere Abwehrmöglichkeiten des Dateninhabers

… durch die „datenschutzrechtliche Hintertür“



- Produktdaten / verbundene Dienstdaten beinhalten personenbezogene Daten, die nicht dem Nutzer zuzuordnen sind => Rechtsgrundlage im Sinne von Art. 6 DSGVO für Verarbeitung erforderlich.
- DA selbst stellt keine Rechtsgrundlage bereit, vgl. Art. 6 Abs. 12 DA.

Weitere Abwehrmöglichkeiten des Dateninhabers

…durch Verzögerung des Verfahrens

- Beispiel:
  - (Hohe) Anforderungen an Nachweis der „Nutzereigenschaft“ (Art. 4 Abs. 5 DA) und „Betroffeneneigenschaft“ (Art. 4 Abs. 12 DA) stellen.
  - (Längeres) Aushandeln von TOMs mit dem Nutzer (Art. 4 Abs. 6 DA).
- Zu beachten: Bußgeldrisiko!

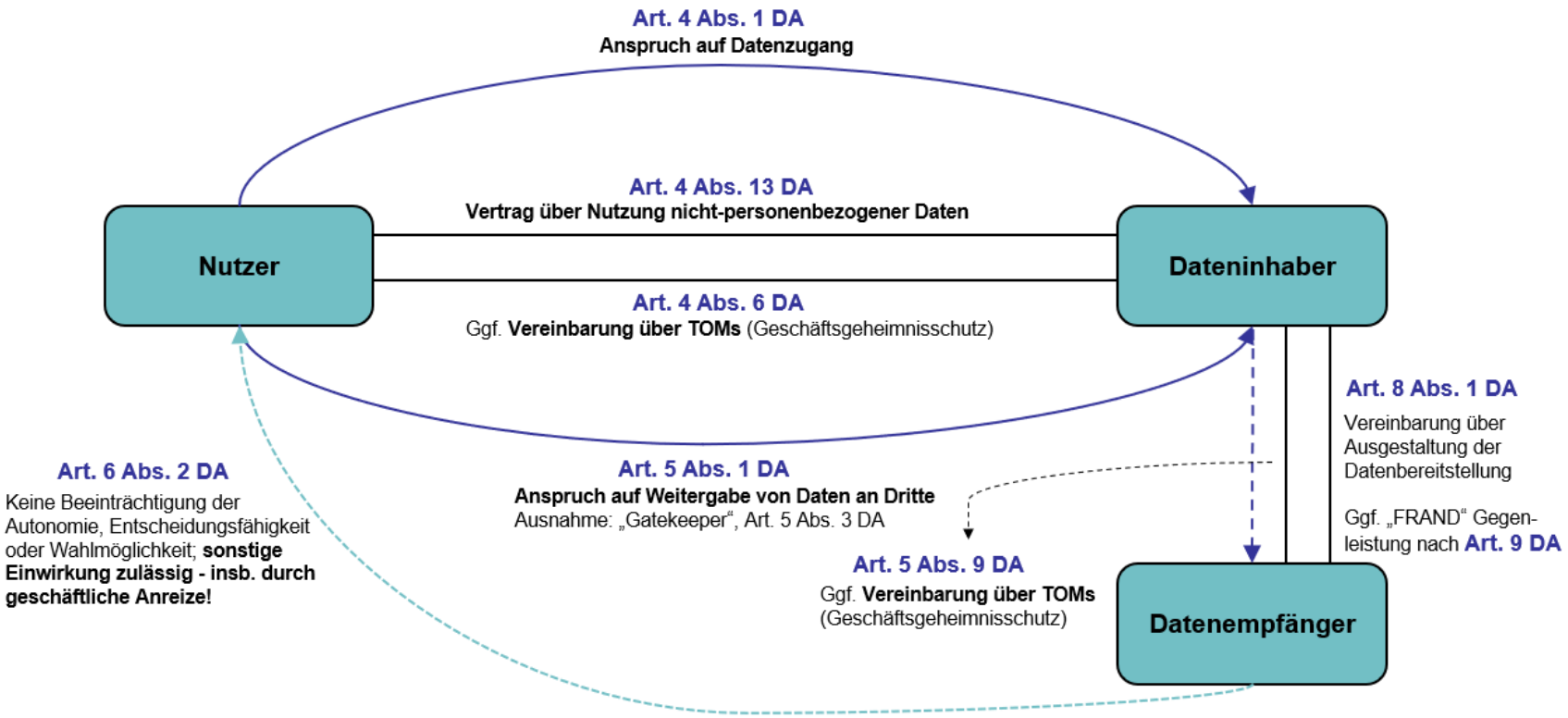
Reaktion des Nutzers

- Nutzer kann bei Zugangsverweigerung
  - **Gericht** anrufen
  - Zusätzlich in den Fällen des Art. 4 Abs. 2 DA (Sicherheit) oder 4 Abs. 7 und 8 (Geheimnisschutz):
    1. **Beschwerde bei der zuständigen Aufsichtsbehörde** einlegen, die dann über Zugang entscheidet (Art. 4 Abs. 3 lit. a / Art. 4 Abs. 9 lit. a DA iVm Art. 37 Abs. 5 lit. b DA).
    2. Mit dem Dateninhaber vereinbaren, eine **Streitbeilegungsstelle** anzurufen (Art. 4 Abs. 3 lit. b / Art. 4 Abs. 9 lit. b DA).

(3) Schutz von Geschäftsgeheimnissen im Verhältnis Datenempfänger vs. Dateninhaber

Verhältnis: Datenempfänger vs. Dateninhaber

- **Weitergabe von Daten an Dritte auf Verlangen des Nutzers, Art. 5 Abs. 1 DA**
  - Ausnahme: Keine Weitergabe an sog. „Gatekeeper“, Art. 5 Abs. 3 DA



Verhältnis: Datenempfänger vs. Dateninhaber

- Weitgehender Gleichlauf mit Art. 4 DA im Hinblick auf:
  - **Zugangsbeschränkungen**
    - Geschäftsgeheimnisschutz, Art. 5 Abs. 9-11 DA
    - Datenschutz, Art. 5 Abs. 7, 8 DA
  - **Nutzungsbeschränkungen**
    - Entwicklung von Konkurrenzprodukten und Ausspähen, Art. 6 Abs. 2 lit. e DA
    - Negative Auswirkung auf Sicherheit des IoT-Produkts oder verbundenen Dienstes, Art. 6 Abs. 2 lit. f DA
  - **Verzögerung des Verfahrens**

Verhältnis: Datenempfänger vs. Dateninhaber

- Gegenüber Dritten muss der Dateninhaber geschäftsgeheimnisrelevante Daten nur in dem Umfang zugänglich machen, wie dies zur Erfüllung des zwischen dem Nutzer und dem Dritten vertraglich vereinbarten Zwecks **unbedingt erforderlich** ist, Art. 5 Abs. 9 DA.

- Bei Verwendung der Daten zur Entwicklung eines Konkurrenzproduktes kann der Dateninhaber von dem Dritten bzw. dem Datenempfänger gemäß Art. 11 Abs. 2 DA u.a. verlangen:
  - **Löschung der Daten**,
  - **Vernichtung der rechtsverletzenden Waren,** sowie
  - **Schadensersatz**.

Reaktion des Datenempfängers

- Weitgehender Gleichlauf - Datenempfänger kann bei Ablehnung der Datenweitergabe:
  - **Gericht** anrufen
  - Zusätzlich in den Fällen des Art. 5 Abs. 10 und 11 (Geheimnisschutz):
    1. **Beschwerde einlegen bei der zuständigen Aufsichtsbehörde**, die dann über die Weitergabe der Daten entscheidet (Art. 4 Abs. 3 lit. a / Art. 4 Abs. 9 lit. a DA iVm Art. 37 Abs. 5 lit. b DA).
    2. Mit dem Dateninhaber vereinbaren, eine **Streitbeilegungsstelle** anzurufen (Art. 4 Abs. 3 lit. b / Art. 4 Abs. 9 lit. b DA).

(4) Umsetzung des DA

Vorbereitung für den Tag X

1 Analyse und Klassifizierung von Daten

- Bestandsaufnahme: Welche Daten werden erlangt, generiert oder erhoben? Was sind das für Daten? Enthalten die Daten Geschäftsgeheimnisse? Wo „liegen“ diese Daten?
- Verantwortlichkeiten bestimmen: Einrichten einer (fachgebietsübergreifenden) Task Force, die relevante Informationen sammelt und Prozesse erarbeitet.

2 Benutzerverwaltung / Prozesse konzipieren

- Identifizierung von Nutzern und ggf. Dritten.
- Aufsetzen eines Entscheidungsprozesses: Wer bearbeitet und entscheidet mit wem und auf welcher Grundlage über Datenzugangsverlangen?
- Prozess für die Verweigerung von Datenzugangsansprüchen erarbeiten.

3 Eigene Nutzung definieren

- Eigene Verwendungszecke und Nutzungsmöglichkeiten mit der Fachabteilung klären, definieren und dokumentieren.

4 Nutzungsbedingungen

- Datenlizenzvereinbarung vorbereiten.
- Nutzungsbedingungen erstellen (einschließlich NDA).
- TOMs (vor-)definieren.