

Das Verweigerungs- und Aussetzungsrecht im Data Act Werden Geschäftsgeheimnisse im Data Act ausreichend geschützt?

Etienne Wolf

Universität Bonn / For:Tech / Scheja & Partners

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Richtlinie bezeichnet der Ausdruck

1. „Geschäftsgeheimnis“ Informationen, die alle nachstehenden Kriterien erfüllen:
 - a) Sie sind in dem Sinne geheim, dass sie weder in ihrer Gesamtheit noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne weiteres zugänglich sind;
 - b) sie sind von kommerziellem Wert, weil sie geheim sind;
 - c) sie sind Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen durch die Person, die die rechtmäßige Kontrolle über die Informationen besitzt;

Legaldefinition in Art. 2 Nr. 1 RL (EU) 2016/943

Verweis in Art. 2 Nr. 18 DA, Umsetzung der Richtlinie 2016/943 in Deutschland durch das 2019 erlassene Geschäftsgeheimnisgesetz

Agenda

- ▶ Veränderungen durch den Data Act
- ▶ Datenzugang im Data Act
- ▶ Aussetzungs- und Verweigerungsrechte des Dateninhabers
- ▶ Ausblick

Rechtsslage vor dem Data Act und neue Herausforderungen

VERÄNDERUNGEN DURCH DEN DATA ACT

Rechtslage vor dem Data Act

- ▶ Erlaubnistatbestände in § 3 Abs. 1 GeschGehG für die Erlangung von Geschäftsgeheimnissen
 - ▶ Eigenständige Entdeckung oder Schöpfung
 - ▶ Reverse Engineering bei öffentlicher Verfügbarmachung des Produkts oder bei rechtmäßigem Besitz
 - ▶ Ausübung von Arbeitnehmerrechten
- ▶ Handlungsverbote in § 4 GeschGehG
 - ▶ Unbefugter Zugang, Aneignung, Kopieren von Informationen, die unter der Kontrolle des Geschäftsgeheimnisinhabers stehen
 - ▶ Sonstige Verhaltensweisen, die gegen die Grundsätze von Treu und Glauben verstoßen
- ▶ Tatbestände beziehen sich nur auf die Erlangung von Geschäftsgeheimnissen, nicht auf die Nutzung und Verwertung
- ▶ Öffnungsklausel in § 3 Abs. 2 GeschGehG für die Erlangung, Nutzung und Offenlegung

Neue Herausforderungen für Geschäftsgeheimnisinhaber

- ▶ Data Act schafft Zugangsrechte für vom Nutzer generierte Daten für den Nutzer von vernetzten Produkten und Dritte
- ▶ Keine exklusive Entscheidungsgewalt des Geschäftsgeheimnisinhabers mehr
- ▶ Schutz von Geschäftsgeheimnissen nach Maßgabe der Richtlinie 2016/943 soll gewahrt werden (Erwägungsgrund 31 DA)
- ▶ Der Data Act schafft eigene Schutzmechanismen, deren Wirksamkeit Aufarbeitung bedarf

Rohdaten als Geschäftsgeheimnisse

- ▶ Datenbegriff im Data Act
 - ▶ Legaldefinition in Art. 2 Nr. 1 DA
 - ▶ Wortgleich zur Definition im DGA und DMA
 - ▶ Ausschließliche Erfassung von digitalen Daten
 - ▶ Rohdaten sind erfasst (Erwägungsgrund 15 DA)
- ▶ Einstufung von Rohdaten als Information, die Geschäftsgeheimnisse beinhalten kann
 - ▶ Erforderlich, um Schutz zu gewährleisten
 - ▶ Gesamtheit der generierten Daten als Geschäftsgeheimnis
 - ▶ Zumindest potentiell wirtschaftlicher Wert

Art. 3 Abs. 1, Art. 4 Abs. 1, Art. 5 Abs. 1 DA

DATENZUGANG IM DATA ACT

Zugangsansprüche im Data Act

- ▶ Zugang by Design, Art. 3 Abs. 1 DA
 - ▶ Kein eigenständiger Zugangsanspruch
 - ▶ Verpflichtung der Hersteller und Anbieter zu Access by Design
 - ▶ Frage der Anwendbarkeit der Schutzvorschriften der Art. 4, 5 DA für den Geschäftsgeheimnisschutz
- ▶ Zugangsanspruch des Nutzers, Art. 4 Abs. 1 DA
 - ▶ Fehlender Zugang gem. Art. 3 DA als Voraussetzung
 - ▶ Geltendmachung des Anspruchs durch einfaches Verlangen
 - ▶ Zugang zu Daten einschließlich der zur Nutzung erforderlichen Metadaten
- ▶ Zugangsanspruch des Dritten, Art. 5 Abs. 1 DA
 - ▶ Bereitstellung der Daten zu FRAND-Bedingungen gem. Art. 8 DA
 - ▶ Gegenleistung gem. Art. 9 DA

Einschränkungen des Datenzugangs

- ▶ Erforderliche Schutzmaßnahmen gem. Art. 4 Abs. 6 DA
 - ▶ Expliziter Schutz von Geschäftsgeheimnissen, werden „gewahrt“
 - ▶ Verpflichtung von Nutzer und Dateninhaber
 - ▶ z.B. Mustervertragsklauseln und Vertraulichkeitsvereinbarungen
 - ▶ Einstufung von Daten als Geschäftsgeheimnis durch Geschäftsgeheimnisinhaber
 - ▶ Angemessenheitsgrundsatz der Schutzmaßnahmen
 - ▶ Erforderlichkeit der Schutzmaßnahmen und Wahrung der Angemessenheit als Herausforderung für Dateninhaber

- ▶ Erforderliche Schutzmaßnahmen gem. Art. 5 Abs. 9 DA
 - ▶ Erforderliche Maßnahmen sind wortlautidentisch zu Art. 4 Abs. 6 DA
 - ▶ Begrenzte Offenlegungspflicht
 - ▶ Für den zwischen Nutzer und Drittem vereinbarten Zweck erforderlich
 - ▶ Zweck wird von Nutzer und Drittem bestimmt, kein Einfluss des Dateninhabers
 - ▶ Steigendes Risiko der Offenlegung bei Einbindung von Dritten
 - ▶ Verweigerungsrecht bei weit gefasstem Zweck?
 - ▶ Enge Auslegung der unbedingt erforderlichen Daten in Art. 5 Abs. 9 DA geboten

Art. 4 Abs. 7, 8 DA, Art. 5 Abs. 10, 11 DA

AUSSETZUNGS- UND VERWEIGERUNGSRECHTE

Art. 4 Abs. 7 DA

(7) Wenn keine Einigung über die in Absatz 6 genannten erforderlichen Maßnahmen erzielt wird oder wenn vom Nutzer die gemäß Absatz 6 vereinbarten Maßnahmen nicht umgesetzt werden oder die Vertraulichkeit der Geschäftsgeheimnisse verletzt wird, kann der Dateninhaber die Weitergabe von Daten, die als Geschäftsgeheimnisse eingestuft wurden, verweigern oder gegebenenfalls aussetzen. Die Entscheidung des Dateninhabers ist ordnungsgemäß zu begründen und dem Nutzer unverzüglich schriftlich mitzuteilen. In solchen Fällen teilt der Dateninhaber der gemäß Artikel 37 benannten zuständigen Behörde mit, dass er die Weitergabe von Daten verweigert oder ausgesetzt hat, und gibt an, welche Maßnahmen nicht vereinbart oder umgesetzt wurden und bei welchen Geschäftsgeheimnissen die Vertraulichkeit untergraben wurde.

Aussetzungs- und Verweigerungsrecht gemäß Art. 4 Abs. 7, Art. 5 Abs. 10 DA

- ▶ Kopplung an Nutzerverhalten
- ▶ Keine Anwendbarkeit bei unverhältnismäßig hohen Hürden für den Datenzugriff
- ▶ Verweigerungsrecht
 - ▶ Bei fehlender Einigung über Schutzmaßnahmen im Sinne des Art. 4 Abs. 6 DA, Art. 5 Abs. 9 DA
 - ▶ ex-ante Betrachtung
 - ▶ Verweigerung des Nutzers/Dritten, die zum Schutz des Geschäftsgeheimnisses erforderlichen Maßnahmen einzuhalten bzw. umzusetzen
 - ▶ z.B. keine Unterzeichnung einer Vertraulichkeitsvereinbarung, Nicht-Akzeptanz der Art des Datenzugangs
 - ▶ Keine Vorlage einer gleichwertigen Alternative

- ▶ Aussetzungsrecht
 - ▶ Wirksame Vereinbarung zwischen Nutzer/Drittem und Dateninhaber
 - ▶ Fehlende Umsetzung der vereinbarten Maßnahmen
 - ▶ Verletzung der Vertraulichkeit des Geschäftsgeheimnisses
- ▶ Rechtsfolge einer Verweigerung / Aussetzung
 - ▶ Unverzögliche, schriftliche Information des Nutzers/Dritten
 - ▶ Ordnungsgemäße Begründung erforderlich
 - ▶ Beweislast liegt beim Dateninhaber
 - ▶ Information der zuständigen Behörde
 - ▶ Durch die Information der Behörde wird einer ausufernden Nutzung entgegengewirkt

Art. 4 Abs. 8 DA

(8) Wenn unter außergewöhnlichen Umständen der Dateninhaber, der Inhaber eines Geschäftsgeheimnisses ist, nachweisen kann, dass er trotz der vom Nutzer gemäß Absatz 6 des vorliegenden Artikels getroffenen technischen und organisatorischen Maßnahmen mit hoher Wahrscheinlichkeit einen schweren wirtschaftlichen Schaden durch die Offenlegung von Geschäftsgeheimnissen erleiden wird, kann er ein Datenzugangsverlangen für die betreffenden speziellen Daten im Einzelfall ablehnen. Dieser Nachweis ist auf der Grundlage objektiver Fakten, insbesondere der Durchsetzbarkeit des Schutzes von Geschäftsgeheimnissen in Drittländern, der Art und des Vertraulichkeitsgrads der verlangten Daten sowie der Einzigartigkeit und Neuartigkeit des vernetzten Produkts hinreichend zu begründen und dem Nutzer unverzüglich schriftlich vorzulegen. Verweigert der Dateninhaber die Weitergabe von Daten gemäß vorliegendem Absatz, so teilt er dies der gemäß Artikel 37 benannten zuständigen Behörde mit.

Verweigerungsrecht gem. Art. 4 Abs. 8, Art. 5 Abs. 11 DA

- ▶ Ergibt sich aus der Eigenschaft eines Datums als Geschäftsgeheimnis
- ▶ Schwerer wirtschaftlicher Schaden durch die Offenlegung der Daten erwartbar
 - ▶ Irreparable wirtschaftliche Verluste
 - ▶ De facto Bedrohung der wirtschaftlichen Existenz
- ▶ Hohe Wahrscheinlichkeit des Schadenseintritts trotz Schutzmaßnahmen
- ▶ Nachweisbare Fakten als Grundlage
- ▶ Faktisch geringer Anwendungsspielraum
 - ▶ Schwerer wirtschaftlicher Schaden durch eine individuelle Datenherausgabe kaum begründbar
 - ▶ Wortlaut und Telos sprechen gegen eine breite Anwendbarkeit
 - ▶ Anwendung nur bei wenigen Sonderfällen
- ▶ Informationspflichten ggü Nutzer und Dateninhaber parallel zu Art. 4 Abs. 7, Art. 5 Abs. 9 DA

Anwendbarkeit der Aussetzungs- und Verweigerungsrechte beim Datenzugriff by Design, Art. 3 Abs. 1 DA

- ▶ Keine Normierung von Aussetzungs- und Verweigerungsrechten in Art. 3 DA
- ▶ Schutzbedürfnis für Geschäftsgeheimnisse besteht jedoch unabhängig von der Art des Datenzugangs
- ▶ Schutz vor (potentieller) Offenlegung von Geschäftsgeheimnissen
- ▶ Fehlender Schutz könnte zu bewusst komplexem Design führen, um sich auf fehlende Durchführbarkeit des Datenzugriffs berufen zu können
- ▶ Anwendbarkeit der Aussetzungs- und Verweigerungsrechte anzunehmen

AUSBLICK

Ausblick

- ▶ Herausforderungen bei der Einstufung von Daten als Geschäftsgeheimnis
 - ▶ Ausufernde Einstufung von Daten als Geschäftsgeheimnisse möglich
 - ▶ Abwägung von Erforderlichkeit und Angemessenheit
- ▶ In-situ-Zugriff als Lösungsansatz?
- ▶ Weitgehende Zugangsansprüche bei geringen Beschränkungsmöglichkeiten
- ▶ Hohe Anforderungen für die Verweigerung und Aussetzung des Datenzugangs
- ▶ Weitere Konkretisierung durch die Rechtsprechung

Vielen Dank für Ihre Aufmerksamkeit

Für Rückfragen stehe ich gerne zur Verfügung:

Etienne Wolf

etienne.wolf@scheja-partners.de

s3etwolf@uni-bonn.de