**Dr. Anette Gärtner** (l.), LL.M. (Edin.), RAin/FAinGewRS sowie Solicitor (England/Wales), ist Partnerin bei Eversheds Sutherland in Frankfurt a. M. Sie ist Expertin für Fragen des Know-how-Schutzes und des Patentrechts, inklusive Arbeitnehmererfindungen.
**Luise Antonie Oppermann** (r.), LL.M. (Emory), ist Referendarin am LG Darmstadt und arbeitet als Wissenschaftliche Mitarbeiterin bei Eversheds Sutherland in Frankfurt a. M. Der Schwerpunkt ihrer Tätigkeit liegt auf dem Gewerblichen Rechtsschutz.

# Ganz großes Tennis? Data Act und Geheimnisschutz

Lange dauert es nicht mehr: Ab September 2025 finden die meisten Regelungen des Data Act („DA") Anwendung (VO (EU) 2023/2854 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung). Einzelne Vorschriften sind gemäß Art. 50 DA erst ab dem 12.9.2026 bzw. ab dem 12.9.2027 anwendbar; im Übrigen gilt die Verordnung ab dem 12.9.2025. Die Europäische Kommission meint, mit dem Data Act habe sie sich auf der Rangliste der Regulierer ganz weit nach vorne gespielt und die Grundlagen für eine „starke, innovative und souveräne europäische Digitalwirtschaft" geschaffen (Binnenmarkt-Kommissar *Thierry Breton*, 2022). Im Unterschied zur KI-Verordnung erhält der Data Act bislang relativ wenig Aufmerksamkeit (vgl. aber *Heinzke*, Die Erste Seite, BB Heft 12/2025). Das verwundert nicht zuletzt angesichts des Aufwandes, der für viele Unternehmen mit der Beachtung der neuen Regeln verbunden sein wird. Mancher wird sich an die DSGVO (VO (EU) 2016/679) erinnert fühlen.

Der Data Act betrifft zwei unterschiedliche Regelungskomplexe. Er befasst sich zum einen mit dem „Cloud Switching", also den Rahmenbedingungen für den Wechsel zwischen Datenverarbeitungsdiensten. Zum anderen will der Data Act sicherstellen, dass die Nutzer sog. vernetzter Produkte oder verbundener Dienste Zugriff auf die Daten erhalten, die bei der Nutzung der Produkte bzw. Dienste generiert werden (Erwägungsgrund 5 DA). Diese Daten sollen sie auch an Dritte weitergeben können, damit diese z. B. das vernetzte Produkt warten können (Erwägungsgrund 15 DA). Was sich sperrig liest, kann erhebliche Auswirkungen haben in einer Welt, in der fast jedes Produkt mit dem Internet verbunden ist. Nicht nur die Vertragswerkstatt, sondern auch die Konkurrenz soll Zugriff auf Daten erhalten, die das internetfähige Auto sammelt, damit der Nutzer die freie Wahl hat, wen er mit der Reparatur beauftragt.

*Spiel, Satz und Geheimnisverlust? Höchste Zeit, sich auf den Data Act vorzubereiten.*

Deswegen verpflichtet Art. 3 Abs. 1 DA die Hersteller vernetzter Produkte, diese von vornherein so zu entwerfen, dass die Produktdaten für den Nutzer direkt zugänglich sind. Diese Pflicht gilt für vernetzte Produkte, die nach dem 12.9.2026 in den Verkehr gebracht werden (Art. 50 DA), bereitet den Betroffenen aber schon jetzt Kopfschmerzen. Denn Art. 3 Abs. 1 DA verursacht Aufwand und rechtliche Unsicherheiten. Die „Access by design"-Vorgabe gemäß Art. 3 Abs. 1 DA wird durch Ansprüche des Nutzers flankiert. Kann der Nutzer nicht direkt auf die Produktdaten zugreifen, so muss der Dateninhaber ihm die ohne Weiteres verfügbaren Daten bereitstellen (Art. 4 Abs. 1 DA). Eine einfache Anfrage genügt. Alternativ steht es dem Nutzer frei, sich eines Dritten zu bedienen (bspw. einer Werkstatt), der die Datenbereitstellung fordert (Art. 5 Abs. 1 DA). Damit verschiebt sich die Datenherrschaft vom Dateninhaber zum Nutzer, zumal der Dateninhaber beim Nutzer um eine Lizenz nachsuchen muss, wenn er die Daten z. B. zur Produktweiterentwicklung verwenden will (Art. 4 Abs. 13 DA).

Was ist mit etwaigen Geschäftsgeheimnissen, die Teil der Produktdaten sein könnten? Auf vielfaches Drängen der Industrie wurden gegen Ende des Gesetzgebungsprozesses noch einige Regeln zum Geheimnisschutz eingefügt. Diese bleiben allerdings hinter den Erwartungen zurück. Im Wesentlichen gleichlautende Unterabsätze der Art. 4 und 5 DA betonen, dass Geschäftsgeheimnisse gewahrt werden sollen. Der Mechanismus ist jedoch denkbar kompliziert. Es genügt nicht, dass der Dateninhaber „Halt, meine Geschäftsgeheimnisse sind betroffen!" einwendet. Nachdem der Nutzer (bzw. Dritte) die Datenbereitstellung gefordert hat, soll der Dateninhaber vielmehr die Geschäftsgeheimnisse identifizieren und sich mit dem Nutzer (bzw. Dritten) auf angemessene Geheimhaltungsmaßnahmen verständigen, wie z. B. ein NDA oder technische Schutzmaßnahmen (Art. 4 Abs. 6, 5 Abs. 9 DA). Nur dann, wenn keine Einigung zustande kommt oder der Nutzer/Dritte sich nicht an die Vereinbarung hält, darf der Dateninhaber die Weitergabe von Daten verweigern. Seine Entscheidung muss er schriftlich begründen und die für die Durchführung des DA zuständige Behörde informieren (Art. 4 Abs. 7, 5 Abs. 10 DA). Die Kommission bezeichnet diesen Mechanismus in ihrem „FAQ, Data Act"-Dokument (Version 1.2 vom 3.2.2025) als „Trade secret handbrake" (S. 7, Nr. 4).

Welche Regeln gelten in Bezug auf Daten, deren Bereitstellung nicht verlangt wird, weil sie ohnehin im Einklang mit Art. 3 Abs. 1 DA direkt zugänglich sind? Die Literatur geht ganz überwiegend davon aus, dass es für diese Daten keinen Geheimnisschutz gibt (statt vieler *Determann*, in: Specht/Hennemann, Data Act/Data Governance Act, 2. Aufl. 2025, DA Art. 3, Rn. 57; *Schmidt-Kessel*, MMR 2024, 75, 80). Anderer Ansicht ist die Kommission, die in den FAQ meint, durch vertragliche Vereinbarungen könne der Datenzugriff unter den Vorbehalt ausreichenden Geheimnisschutzes gestellt werden. Sprich: Die „Trade secret handbrake" soll auch bei direkt zugänglichen Daten helfen (FAQ, S. 18, Nr. 24). Diese Position scheint schwer vereinbar mit Art. 7 Abs. 2 DA. Danach sind Vertragsklauseln unwirksam, welche die Rechte des Nutzers einschränken. Möglicherweise ist die Kommission der Ansicht, die „Access by design"-Verpflichtung des Art. 3 Abs. 1 DA sei zwar drittschützend, gebe dem Nutzer aber kein Recht im Sinne des Art. 7 Abs. 2 DA. Man weiß es nicht. Die letztverbindliche Interpretation wird der EuGH liefern müssen.

Manche schlagen daher durchaus pragmatisch vor, technische Schutzmaßnahmen zu ergreifen, damit Produktdaten nicht direkt zugänglich sind (*Determann*, a. a. O.; *Grützmacher*, Data Act, Kölner Tage IT-Recht, 13.3.2025). Dafür spricht auf den ersten Blick, dass der Data Act keine Sanktion für die Nicht-Einhaltung des Art. 3 Abs. 1 androht. Zu beachten sind allerdings auch die nationalen Gesetze. Als Beispiel sei der Entwurf eines „Data Act-Durchführungsgesetzes" vom 7.2.2025 genannt. Dieser RefE ist zwar aufgrund der vorgezogenen Bundestagswahl am 23.2.2025 dem Grundsatz der Diskontinuität zum Opfer gefallen. Da es zur Durchsetzung des DA durch die Bundesnetzagentur flankierender Regelungen bedarf und bis zum 12.9.2025 nicht mehr viel Zeit verbleibt, wird der Entwurf aber vermutlich den Weg ins Gesetzgebungsverfahren finden. § 18 Abs. 3 Nr. 1 des RefE sieht für einen Verstoß gegen Art. 3 Abs. 1 DA eine Geldbuße von bis zu 50.000 Euro vor. Wer die Pflicht nach Art. 3 Abs. 1 DA ignoriert, geht ein kalkuliertes Risiko ein. Sicheren Schutz gegen den Geheimnisverlust bietet also nur eine radikale Maßnahme, die selten in Betracht kommen wird: Vernetzte Produkte so entwerfen, dass sie weniger Daten sammeln.