



Datenverträge im Spannungsfeld zwischen DSGVO und Data Act

ANTONIA STOLL



Gefördert durch:



Bundesministerium
für Wirtschaft
und Energie

Mittelstand-
Digital

aufgrund eines Beschlusses
des Deutschen Bundestages

In diesem Nachgelesen erfahren Sie

- wie DSGVO und Data Act als zwei Regelwerke mit komplementären Funktionen zusammenspielen,
- welche neuen Rechte und Pflichten entstehen und wo ein Spannungsverhältnis zur DSGVO besteht,
- welche Herausforderungen in der Praxis auftreten,
- welche Ansätze zur Konfliktlösung diskutiert werden und
- warum der Datenvertrag als Brücke zwischen DSGVO und Data Act gilt.

Impressum

HERAUSGEBER

Mittelstand-Digital Zentrum Chemnitz
c/o TU Chemnitz
Erfenschlager Str. 73, 09125 Chemnitz
Tel: 0371 531 19935 Fax: 0371 531 819935
info@digitalzentrum-chemnitz.de
www.digitalzentrum-chemnitz.de

REDAKTION Anikó Lessi

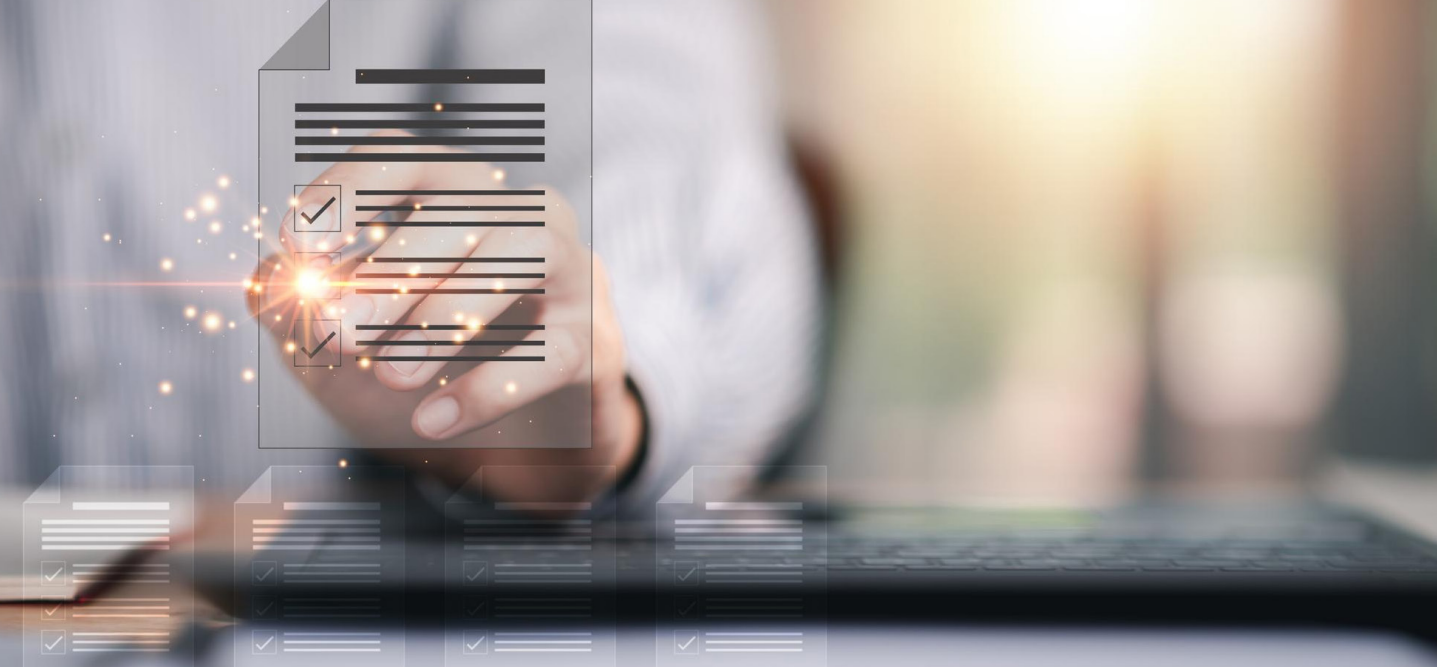
GESTALTUNG UND PRODUKTION

PUNKT191 – Marketing und Design
www.punkt191.de

BILDNACHWEIS TITEL Antonia Stoll (generiert mit KI)

VERÖFFENTLICHUNG Oktober 2025





↑ © abuuhurera – Freepik.com

Daten sind ein zentraler Rohstoff der digitalen Wirtschaft. Doch anders als physische Güter unterliegen sie keinem klar geregelten Eigentumsregime.^[1] Stattdessen bestimmen gesetzliche Vorgaben und vertragliche Vereinbarungen, wer Daten nutzen darf und zu welchem Zweck. In der Europäischen Union treten dabei zwei zentrale Rechtsakte in den Vordergrund: die Datenschutz-Grundverordnung (DSGVO) und der Data Act (EU-VO 2023/2854). Beide verfolgen unterschiedliche Zielrichtungen, bilden jedoch im Zusammenspiel den Rahmen für einen rechtssicheren und innovationsfördernden Umgang mit Daten.

Für Unternehmen – insbesondere kleine und mittlere Unternehmen (KMU) – ergibt sich daraus eine erhebliche Herausforderung: Wie lässt sich der strenge Datenschutz der DSGVO mit den neuen Chancen und Pflichten des Data Acts in Einklang bringen? Ein möglicher Lösungsansatz liegt im Konzept des Datenvertrags.

raler Grundsatz bleibt: Ohne Rechtsgrundlage keine Verarbeitung.

Der Data Act ist am 11.1.2024 in Kraft getreten und gilt überwiegend ab dem 12.9.2025, s. Art. 50 DA.^[2] Im Gegensatz zur DSGVO verfolgt er das Ziel, den Zugang zu Daten zu erleichtern und deren Nutzung für die europäische Wirtschaft zu fördern. Er richtet sich vorrangig auf nicht-personenbezogene Daten, etwa Maschinendaten aus dem Internet der Dinge, kann aber auch personenbezogene Daten betreffen, sofern diese im Kontext vernetzter Produkte anfallen.^[3] In solchen Fällen greift jedoch der Vorrang der DSGVO, s. Art. 1 Abs. 5 DA.^[3]

Damit ergibt sich ein komplementäres Verhältnis: Die DSGVO sichert Privatsphäre und Grundrechte, während der Data Act Innovationshemmnisse abbaut und faire Wettbewerbsbedingungen fördern soll.

DSGVO und Data Act – Zwei Regelwerke mit komplementären Funktionen

Die DSGVO schützt personenbezogene Daten und bestimmt detailliert, unter welchen Voraussetzungen diese verarbeitet werden dürfen. Sie verleiht betroffenen Personen weitreichende Rechte – etwa Auskunft, Berichtigung oder Löschung – und verpflichtet Unternehmen, technische und organisatorische Maßnahmen zum Schutz der Daten zu ergreifen. Zent-

Merke:

- DSGVO = Schutz personenbezogener Daten, klare Pflichten und Rechte.
- Data Act = Zugang zu (nicht-)personenbezogenen Daten, Förderung von Innovation.
- Beide Regelwerke ergänzen sich – DSGVO hat Vorrang, wenn personenbezogene Daten betroffen sind.



Neue Rechte, Pflichten und Spannungsverhältnis zur DSGVO

Mit dem Data Act werden umfassende neue Rechte und Pflichten eingeführt, die die europäische Datenwirtschaft stärken sollen. Nutzer erhalten Zugangs- und Portabilitätsrechte: Sie können auf die durch ihre Geräte erzeugten Daten zugreifen, diese weitergeben und innerhalb von 30 Tagen den Cloud-Anbieter wechseln.^[4] Ergänzend verpflichtet der Data Act Unternehmen zur Datenteilung und führt ein Fairnessgebot für Vertragsklauseln ein, das insbesondere KMU vor einseitigen Benachteiligungen schützt.^[4] Zur Orientierung für eine rechtssichere Vertragsgestaltung sollen zudem Mustervertragsklauseln bereitgestellt werden.

Diese innovationsfreundlichen Regelungen geraten jedoch in ein Spannungsverhältnis mit der DSGVO. Während der Data Act den Datenzugang möglichst weit öffnen will, schützt die DSGVO personenbezogene Daten und schreibt vor: Ohne Rechtsgrundlage keine Verarbeitung.^[4] Da die Zugangsrechte des Data Acts auch personenbezogene Daten erfassen können, gilt in Konfliktfällen stets der Vorrang der DSGVO, vgl. Art. 1 Abs. 5 DA und EW (5) DA. Dies begründet sich aus ihrer höherrangigen Funktion. Die DSGVO dient unmittelbar dem Grundrecht auf Datenschutz (Art. 8 GRCh), während der Data Act primär wirtschafts- und wettbewerbspolitische Ziele verfolgt.^[3]

Merke:

- Nutzer können künftig leichter auf ihre Daten zugreifen und sie weitergeben.
- Cloud-Wechsel innerhalb von 30 Tagen muss gewährleistet sein.
- Unfaire Vertragsklauseln sind nichtig – vor allem KMU profitieren.
- Mustervertragsklauseln helfen bei rechtssicherer Gestaltung.



Herausforderungen in der Praxis

In der Unternehmenspraxis ergeben sich durch die parallele Anwendung beider Regelwerke zahlreiche Konfliktfelder. Ein zentrales Problem ist die Abgrenzung zwischen personenbezogenen und nicht-personenbezogenen Daten. Viele Datensätze enthalten beide Kategorien – beispielsweise Maschinendaten, die über eine Seriennummer einem konkreten Nutzer zugeordnet werden können. Solche „gemischten Datensätze“ erfordern eine besonders sorgfältige Prüfung.^[4]

Besondere Schwierigkeiten bestehen zudem bei der Bestimmung einer tragfähigen Rechtsgrundlage nach Art. 6 DSGVO, wenn personenbezogene Daten von den Datenzugangsrechten erfasst sind. Zwar nennt der Data Act ausdrücklich die Einwilligung oder die Vertragserfüllung als mögliche Anknüpfungspunkte, vgl. EW 34 DA, doch sind diese in der Praxis häufig nur eingeschränkt tauglich.^[5] Realistischer erscheint daher oftmals eine Verarbeitung auf Grundlage berechtigter Interessen, Art. 6 Abs. 1 lit. f DSGVO, die jedoch eine sorgfältige einzelfallbezogene Interessenabwägung erfordert.^[3]

Ein weiteres Problem besteht in der unklaren Rollenverteilung im Data Act. Während die DSGVO strikt zwischen Verantwortlichem und Auftragsverarbeiter unterscheidet, fehlen im Data Act eindeutige Regelungen.^[2] Dies kann zu Unsicherheiten bei der Pflichtenverteilung führen.

Auch die Anonymisierung stellt in der Praxis eine erhebliche Hürde dar. Um Daten aus dem Anwendungsbereich der DSGVO herauszunehmen, muss die Anonymisierung vollständig und unumkehrbar sein – was technisch oft schwer zu erreichen ist. Fehler in diesem Prozess können zu Datenschutzverstößen führen.

Schließlich stehen viele Unternehmen vor der Aufgabe, bestehende Verträge anzupassen. Der Data Act sieht vor, dass bis September 2027 auch ältere Vereinbarungen mit seinen Vorgaben in Einklang gebracht werden müssen.^[2]

Ansätze zur Konfliktlösung

Um die Spannungen zwischen DSGVO und Data Act zu entschärfen, empfiehlt sich ein ganzheitlicher Ansatz, der technische, organisatorische und vertragliche Maßnahmen verbindet.



Eine klare Datenklassifizierung bildet hierbei den ersten Schritt: Unternehmen müssen wissen, welche Daten personenbezogen sind und welche nicht. Technische Trennungen – etwa durch separate Datenbanken oder differenzierte Zugriffsrechte – können helfen, gemischte Datensätze zu vermeiden. Wo möglich, sollte eine konsequente Anonymisierung erfolgen, allerdings nur, wenn sie rechtlich und technisch belastbar ist, vgl. EW 7 DA.^[3] Ein praktikabler Lösungsansatz besteht darin, die vertragliche Ausgestaltung der Datenübermittlung durch den Abschluss eines Datenvertrags zwischen Dateninhaber und Nutzer abzusichern.^[3]

Der Datenvertrag – Brücke zwischen DSGVO und Data Act

Kern eines solchen Vertrags wäre die Verpflichtung des Nutzers, das Vorliegen einer datenschutzrechtlichen Rechtsgrundlage sicherzustellen und hierfür gegenüber dem Dateninhaber einzustehen. Der Datenvertrag fungiert damit als zusätzlicher Schutzmechanismus, der das Risiko des Dateninhabers zwar nicht vollständig beseitigt, aber jedenfalls im Innenverhältnis eine klare Verantwortungszuweisung und einen möglichen Regress eröffnet, vgl. Art. 26 Abs. 1 S. 2 sowie EW 7 und 34 DA.^[3]

Für die Ausgestaltung eines Datenvertrags sind insbesondere drei Punkte von zentraler Bedeutung: Erstens sollten Art und Umfang der zu übermittelnden personenbezogenen Daten sowie die Rollenverteilung der Beteiligten eindeutig festgelegt werden, einschließlich der Zuweisung von Informationspflichten nach Art. 13, 14 DSGVO.^[3]

Zweitens ist die Pflicht des Nutzers zu konkretisieren, die einschlägige Rechtsgrundlage – sei es Einwilligung, s. Art. 6 Abs. 1 lit. a DSGVO, Vertragserfüllung, vgl. Art. 6 Abs. 1 lit. b DSGVO oder berechtigtes Interesse gem. Art. 6 Abs. 1 lit. f DSGVO – nicht nur zu benennen, sondern deren Fortbestand gegenüber dem Dateninhaber laufend sicherzustellen.^[3]

Drittens sollte ein vertragliches Kündigungs- bzw. Suspendierungsrecht des Dateninhabers für den Fall bestehen, dass Zweifel an der Wirksamkeit der gewählten Rechtsgrundlage aufkommen.

Ergänzend bietet sich die Aufnahme detaillierter Haftungsregelungen an, die sowohl Schadensersatzansprüche nach Art. 82 DSGVO als auch mögliche Bußgelder berücksichtigen. Auch wenn Bußgelder grundsätzlich nach individueller Verantwortlichkeit verhängt werden, s. Art. 83 Abs. 2 lit. d DSGVO, erscheint eine vertragliche Regressmöglichkeit im Innenverhältnis sachgerecht, um eine faire Verteilung von Risiken und

Verantwortlichkeiten zu gewährleisten.^[3]

Der Datenvertrag kann damit zwar nicht den Anwendungsvorrang der DSGVO beseitigen, aber er verschafft dem Dateninhaber ein zusätzliches Instrument, um die datenschutzrechtlichen Risiken, die mit der praktischen Umsetzung der Datenzugangsrechte nach dem Data Act verbunden sind, abzumildern und rechtssicher zu strukturieren.

Merke:

- Datenkategorien- und -umfang, Rollen und Informationspflichten festlegen
- Verpflichtung des Nutzers zur Festlegung der Rechtsgrundlage nach Art. 6 DSGVO
- Kündigungs- und Suspendierungsrecht des Dateninhabers bei Zweifeln
- Haftungs- und Regressregelungen nach Art. 82 DSGVO
- Klare Datenklassifizierung und technische Trennung zur Vermeidung gemischter Datensätze



Fazit

Für kleine und mittlere Unternehmen (KMU) bedeutet die Doppelwirkung von Data Act und DSGVO eine besondere Herausforderung. Sie sollen Datenzugangsrechte gewähren und von neuen Marktchancen profitieren, tragen jedoch zugleich ein hohes Risiko für Datenschutzverstöße. Klare Mustervertragsklauseln, technische Trennungen von Datenarten und Datenverträge sind daher zentrale Instrumente, um dieses Spannungsverhältnis beherrschbar zu machen. Nur so können KMU die Chancen des Data Acts nutzen, ohne an den strengen Vorgaben der DSGVO zu scheitern.



Quellen

- 1** M. Hennemann und B. Steinrötter, „Data Act – Fundament des neuen EU-Datenwirtschaftsrechts?“, Neue Juristische Wochenschrift (NJW), p. 1481, 2022.
- 2** P. Zikesch und T. Sörup, „Bestandsvertrag trifft Data Act“, Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT (MMR), p. 487, 2025.
- 3** M. Götz und S. Blöink, „Datenvertrag: Lösungsansatz für das Spannungsfeld zwischen Data Act und DS GVO“, Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT (MMR), p. 451, 2024.
- 4** B. Steinrötter, „Verhältnis von Data Act und DS-GVO“, Gewerblicher Rechtsschutz und Urheberrecht (GRUR), p. 216, 2023.
- 5** S. Assion und L. Willecke, „Der EU Data Act“, Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT (MMR), p. 805, 2023.

Verfasst von

ANTONIA STOLL ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Privatrecht und Recht des geistigen Eigentums der Technischen Universität Chemnitz. Im Mittelstand-Digital Zentrum Chemnitz beschäftigt sie sich mit insbesondere datenschutzrechtlichen Fragen rund um IT und Digitalisierung.

roland.hallau@digitalzentrum-chemnitz.de

Weitere Informationen

Das Mittelstand-Digital Zentrum Chemnitz gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

WAS IST MITTELSTAND-DIGITAL?

Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand-Digital Zentren und der Initiative IT-Sicherheit in der Wirtschaft umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung der Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter www.mittelstand-digital.de.



Gefördert durch:



Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand-Digital 