# Update Deutschland 2025 – Teil III

Herausforderungen zunehmender Regulierung

**Internet of Things (IoT): Neue Regeln für Datenzugang und Datennutzung**

Der Data Act verändert grundlegend den Umgang mit Daten. Untnerhmen müssen sich auf neue Anforderungen und Pflichten einstellen.

—

**DSGVO, KI-Verordnung, Data Act & Co.: Regulatorische Schnittstellen und Herausforderungen**

Mit zunehmender Regulierung entstehen neue Herausforderungen für Unternehmen. Welche Gesetze greifen ineinander – und wo entstehen Konflikte?

—

**Verträge zur Datenverwertung: Rechtliche Rahmenbedingungen und Best Practices**

Klare Regeln zu Eigentum, Nutzung und Sicherheit sind der Schlüssel für eine effiziente Verwertung von Daten.

—

**Compliance-Check: Was Unternehmen im Umgang mit Daten jetzt beachten müssen**

Eine strukturierte Vorgehensweise hilft, Risiken zu vermeiden und die Datenstrategie rechtskonform auszurichten. Welche Maßnahmen jetzt besonders wichtig sind.

—


## Data Act und Künstliche Intelligenz

Liebe Leserinnen und Leser,

Der Data Act der Europäischen Union zielt darauf ab, den Datenmarkt zu regulieren und klare Regeln für den Umgang mit Daten festzulegen.

Parallel dazu entwickelt sich die Künstliche Intelligenz (KI) rasant und gewinnt in Wirtschaft und Gesellschaft an Bedeutung. Auch in diesem Bereich hat der europäische Gesetzgeber durch Inkrafttreten der KI-Verordnung (AI Act) zwar grundsätzlich einen rechtlichen Rahmen geschaffen; dessen praktische Auswirkungen sind jedoch in weiten Teilen noch unklar.

Immer wieder tauchen im Zusammenhang mit ChatGPT, DeepSeek, Mistral & Co. dieselben Fragen auf: Woher kommen die Daten? Wie steht es um den Datenschutz? Und was muss ich in meinem eigenen Unternehmen beachten?

Mit dem dritten und letzten Teil unserer Serie „**Update Deutschland 2025**“ wollen wir Sie auf den aktuellen Stand bringen und versuchen, ein wenig Licht ins Dunkel zu bringen.

Beste Grüße

Prof. Dr. Jochen Bauerreis

# Internet of Things (IoT): Neue Regeln für Datenzugang und Datennutzung


**Der Data Act der Europäischen Union, der am 11. Januar 2024 in Kraft getreten ist und ab dem 12. September 2025 EU-weit direkt anwendbar sein wird, zielt darauf ab, den Zugang zu und die Nutzung von Daten innerhalb der EU zu harmonisieren. Er soll die Datennutzung in verschiedenen Lebensbereichen verbessern und zur Wertschöpfung, insbesondere für neue Geschäftsmodelle, Start-ups und kleine und mittlere Unternehmen (KMU) beitragen.**

Der Data Act umfasst eine Vielzahl von Bestimmungen, die darauf abzielen, den **Datenzugang und die Datennutzung fairer und transparenter** zu gestalten. Dazu gehören Regelungen zur Datenweitergabe von Unternehmen an Verbraucher (B2C) und zwischen Unternehmen (B2B), Pflichten der Dateninhaber bezüglich der Bereitstellung von Daten, das Verbot missbräuchlicher Vertragsklauseln sowie die Bereitstellung von Daten für öffentliche Stellen (B2G) in Notfällen. Zudem legt der Data Act vertragliche und technische Anforderungen für den Wechsel zwischen verschiedenen Datenverarbeitungsdiensten („Cloud Switching") fest.

Ein besonderer Fokus liegt auf dem **Internet of Things (IoT)**. IoT-Produkte (stark vereinfacht: „vernetzte" Produkte) generieren eine enorme Menge an Daten, die sowohl für Unternehmen als auch für Verbraucher von hoher Relevanz sind. Der Data Act stellt sicher, dass Nutzer von IoT-Produkten das Recht haben, auf die von ihnen erzeugten Daten zuzugreifen und diese mit Dritten zu teilen. Dies ermöglicht eine größere Kontrolle über die eigenen Daten und schafft neue Möglichkeiten für Dienstleistungsanbieter, indem sie innovative datengetriebene Lösungen entwickeln können. Gleichzeitig müssen Unternehmen sicherstellen, dass die Verarbeitung und Weitergabe dieser Daten im Einklang mit den Datenschutzrichtlinien und den neuen regulatorischen Anforderungen stehen.

Der Data Act stellt einen bedeutenden Schritt in Richtung eines fairen und transparenten Datenökosystems in der EU dar. Unternehmen sollten die verbleibende Übergangszeit nutzen, um ihre Datenstrategien anzupassen und die notwendigen Maßnahmen zur Einhaltung der neuen Vorschriften zu ergreifen. Durch proaktive Anpassungen können sie nicht nur Compliance sicherstellen, sondern auch die vielfältigen Chancen nutzen, die der Data Act bietet. Besonders im Bereich des IoT bietet der erleichterte Datenzugang Unternehmen die Möglichkeit, neue Geschäftsmodelle zu entwickeln und den digitalen Wandel weiter voranzutreiben.

***Beispiel:***
*Ein Hersteller von vernetzten Haushaltsgeräten wie Smart-Kühlschränken und intelligenten Thermostaten könnte durch den Data Act verpflichtet sein, seinen Kunden Zugang zu den von den Geräten generierten Daten zu gewähren. Bisher wurden diese Daten primär intern genutzt, um Produktverbesserungen und Wartungsservices anzubieten. Durch die neuen Regelungen müssen die Kunden jedoch in die Lage versetzt werden, ihre Gerätedaten auch an Drittanbieter weiterzugeben, beispielsweise an Energiedienstleister für optimierte Stromtarife oder an unabhängige Reparaturservices. Dies eröffnet dem Unternehmen neue Möglichkeiten, etwa durch Partnerschaften mit externen Serviceanbietern, erfordert jedoch zugleich eine Anpassung der internen Datenmanagement- und Sicherheitsstrategien, um den Datenschutz zu gewährleisten und regulatorische Anforderungen zu erfüllen.*

# DSGVO, KI-Verordnung, Data Act & Co.: Regulatorische Schnittstellen und Herausforderungen

**Die Regulierung von Daten und Künstlicher Intelligenz (KI) nimmt in Europa immer weiter zu. Mit der Datenschutz-Grundverordnung (DSGVO), der KI-Verordnung (AI Act der Europäischen Union) und dem Data Act existieren inzwischen mehrere Regulierungswerke, die Unternehmen und Organisationen in ihren digitalen Prozessen berücksichtigen müssen. Doch wie greifen diese Gesetze ineinander, wo gibt es Schnittstellen, und welche Herausforderungen entstehen daraus?**

Obwohl die verschiedenen Rechtsgrundlagen unterschiedliche Aspekte der digitalen Welt regulieren, gibt es zahlreiche Berührungspunkte:

- **Datennutzung und Datenschutz**: Der Data Act erleichtert den Zugang zu nicht-personenbezogenen Daten, muss jedoch mit der DSGVO abgeglichen werden, um sicherzustellen, dass keine personenbezogenen Daten unzulässig weitergegeben werden.
- **KI und Datenschutz**: KI-Systeme sind oft auf große Mengen personenbezogener Daten angewiesen, weshalb Unternehmen die Anforderungen der DSGVO mit den Regelungen der KI-Verordnung in Einklang bringen müssen.
- **Verantwortlichkeit und Compliance**: Unternehmen, die KI-Modelle entwickeln oder nutzen, stehen vor der Herausforderung, sowohl die Transparenzanforderungen der KI-Verordnung als auch die Datenschutzpflichten der DSGVO zu erfüllen.
- **Interoperabilität und Datenzugang**: Der Data Act fordert eine bessere Interoperabilität zwischen verschiedenen Systemen und die Verfügbarkeit von Daten, was wiederum mit der Kontrolle und Zweckbindung in der DSGVO in Konflikt geraten kann.

Die Einhaltung mehrerer sich überschneidender Regulierungsakte stellt Unternehmen vor erhebliche Herausforderungen:

- **Komplexität der Umsetzung**: Unternehmen müssen sicherstellen, dass ihre digitalen Prozesse den Anforderungen aller drei Regulierungen entsprechen, was eine umfassende Compliance-Strategie erfordert.
- **Kostendruck und Ressourcenaufwand**: Die Implementierung neuer Datenschutz- und Transparenzmechanismen verursacht Kosten und benötigt Fachwissen.
- **Haftungsrisiken**: Verstöße gegen die DSGVO, den Data Act oder die KI-Verordnung können empfindliche Strafen nach sich ziehen.
- **Technische Herausforderungen**: Die Anforderung an Datenportabilität und Transparenz setzt oft neue technische Lösungen und IT-Infrastrukturen voraus.

Die regulatorische Landschaft in Europa wird zunehmend komplexer, was Unternehmen sowohl Herausforderungen als auch Chancen bietet. Während die Gesetze den Schutz von Daten und ethische Standards für KI-Systeme sicherstellen, müssen Unternehmen große Anstrengungen unternehmen, um Compliance-Anforderungen zu erfüllen. Ein ganzheitliches Compliance-Management sowie die frühzeitige Anpassung an regulatorische Anforderungen sind der Schlüssel, um langfristig wettbewerbsfähig zu bleiben.

# Verträge zur Datenverwertung: Rechtliche Rahmenbedingungen und Best Practices

**Die wirtschaftliche Bedeutung von Daten nimmt stetig zu, und Unternehmen nutzen sie zunehmend als wertvolle Ressource. Doch um Daten sicher und effizient zu verwerten, sind klare vertragliche Regelungen notwendig. Wir analysieren die rechtlichen Rahmenbedingungen für Verträge zur Datenverwertung und zeigen Best Practices auf, die Unternehmen bei der Gestaltung solcher Verträge beachten sollten.**

Datenverwertungsverträge sind oft komplex, da sie in einem dynamischen rechtlichen Umfeld operieren. Zu den wichtigsten rechtlichen Grundlagen gehören:

- **Datenschutzrecht (DSGVO)**: Die Verarbeitung personenbezogener Daten unterliegt strengen Vorschriften der Datenschutz-Grundverordnung (DSGVO). Unternehmen müssen sicherstellen, dass sie die Zustimmung der betroffenen Personen einholen oder auf eine gesetzliche Grundlage zur Verarbeitung zurückgreifen können.
- **Urheber- und Schutzrechte**: Daten können unter das Urheberrecht, Datenbankrecht oder andere Schutzrechte fallen. Hierbei ist zu klären, wer die Rechte an den Daten besitzt und welche Nutzungsrechte übertragen werden können.
- **Wettbewerbs- und Karttellrecht**: Die gemeinsame Nutzung oder der Verkauf von Daten zwischen Unternehmen könnten wettbewerbsrechtliche Fragen aufwerfen. Kartellrechtliche Vorschriften müssen beachtet werden, um Marktmachtmissbrauch zu vermeiden.
- **Vertragsrecht**: Grundsätze des Vertragsrechts, insbesondere Regelungen zu Haftung, Gewährleistung und Vertragsstrafen, sind essenziell, um Rechtsstreitigkeiten vorzubeugen. Des Weiteren stellt sich die Frage der vertragstypologischen Einordnung (Kaufrecht, Miet- oder Pachtrecht, Dienstvertragsrecht usw.).

## *Best Practices bei der Vertragsgestaltung*

*Um rechtskonforme und effiziente Datenverwertungsverträge zu gestalten, sollten Unternehmen Folgendes berücksichtigen:*

1. ***Klare Definition der Daten**: Der Vertrag sollte genau festlegen, welche Daten genutzt werden, woher sie stammen und in welchem Umfang sie verwendet werden dürfen.*
2. ***Rechte und Pflichten der Vertragsparteien**: Die Vereinbarungen sollten eindeutig regeln, wer welche Verantwortung bei der Datennutzung trägt, insbesondere in Bezug auf Datenschutz und Sicherheit.*
3. ***Nutzungsrechte und Einschränkungen**: Festlegung, ob die Nutzung exklusiv oder nicht-exklusiv erfolgt und ob Dritte auf die Daten zugreifen dürfen.*
4. ***Datenqualität und -sicherheit**: Standards zur Datenintegrität, Verschlüsselung und Speicherung sollten definiert werden, um Compliance-Risiken zu minimieren.*
5. ***Laufzeit und Beendigung**: Regelungen zu Vertragslaufzeit, Kündigungsmöglichkeiten und Datenlöschung nach Vertragsende sollten festgelegt werden.*
6. ***Haftung und Sanktionen**: Es sollte geklärt werden, welche Haftungsregelungen greifen und welche Strafen bei Vertragsverletzungen vorgesehen sind.*

Verträge zur Datenverwertung sind ein essenzieller Bestandteil der modernen Datenwirtschaft. Unternehmen müssen sowohl die rechtlichen Rahmenbedingungen als auch bewährte Vertragspraktiken berücksichtigen, um rechtliche Risiken zu minimieren und den Wert von Daten optimal zu nutzen. Eine fundierte vertragliche Gestaltung ist der Schlüssel zu einer erfolgreichen und rechtssicheren Datenverwertung.

# Compliance-Check: Was Unternehmen im Umgang mit Daten jetzt beachten müssen


**Daten sind für Unternehmen eine wertvolle Ressource, aber auch eine potenzielle rechtliche Herausforderung. Mit der zunehmenden Regulierung durch Gesetze wie die Datenschutz-Grundverordnung (DSGVO), den Data Act und die KI-Verordnung steigen die Anforderungen an den verantwortungsvollen Umgang mit Daten. Unternehmen müssen sicherstellen, dass sie alle relevanten Vorschriften einhalten, um rechtliche Risiken zu minimieren. Ein strukturierter Compliance-Check ist dabei unerlässlich.**

Unternehmen sollten folgende Schritte in ihren Compliance-Check integrieren:

- ✓ **Bestandsaufnahme und Dateninventur**: Unternehmen sollten zunächst eine vollständige Erfassung ihrer gesammelten, verarbeiteten und gespeicherten Daten durchführen. Dazu gehört die Identifizierung personenbezogener und nicht-personenbezogener Daten sowie eine detaillierte Analyse, welche Systeme und Prozesse mit diesen Daten arbeiten.

- ✓ **Risikobewertung und Datenschutz-Folgenabschätzung**: Eine umfassende Risikobewertung sollte durchgeführt werden, um potenzielle Datenschutzverletzungen oder Sicherheitsrisiken zu identifizieren. Für kritische Verarbeitungen personenbezogener Daten ist eine Datenschutz-Folgenabschätzung (DSFA) nach DSGVO erforderlich.

- ✓ **Maßnahmen definieren und implementieren**: Unternehmen sollten technische und organisatorische Maßnahmen zur Sicherstellung der Compliance festlegen. Dazu gehören Datenverschlüsselung, Zugriffskontrollen, Regelungen zur Datenminimierung sowie Schulungen für Mitarbeiter.

- ✓ **Schulung und Sensibilisierung**: Datenschutz und Datensicherheit sind nicht allein eine Aufgabe der IT-Abteilung. Mitarbeiter in allen relevanten Bereichen müssen geschult werden, um den sicheren und rechtskonformen Umgang mit Daten zu gewährleisten.

- ✓ **Regelmäßige Überprüfung und Audits**: Compliance-Maßnahmen müssen kontinuierlich überprüft und aktualisiert werden. Unternehmen sollten regelmäßig interne Audits durchführen, um sicherzustellen, dass sie sich an aktuelle rechtliche Vorgaben halten und potenzielle Sicherheitslücken frühzeitig erkennen.

- ✓ **Verantwortlichkeiten klären**: Es sollte festgelegt werden, wer innerhalb des Unternehmens für die Einhaltung der verschiedenen regulatorischen Anforderungen verantwortlich ist. Datenschutzbeauftragte oder Compliance-Manager können eine zentrale Rolle bei der Umsetzung und Kontrolle der Maßnahmen spielen.

- ✓ **Notfallmanagement und Reaktionsstrategien**: Unternehmen sollten klare Prozesse für den Umgang mit Datenschutzverletzungen und Sicherheitsvorfällen haben. Dies beinhaltet ein effektives Meldewesen sowie ein Kommunikationskonzept für betroffene Nutzer und Aufsichtsbehörden.

***Haben Sie Rückfragen? Für weitere Informationen zu den oben genannten Themen oder für individuelle Beratungsanfragen stehen wir Ihnen selbstverständlich gerne zur Verfügung.***

*Unsere internationale Rechtsanwaltskanzlei ABCI ALISTER mit Standorten in Straßburg & Kehl sowie in Paris, Lyon, Nizza, Montpellier und Montélimar berät Unternehmen in allen Bereichen des internationalen, deutschen und französischen Wirtschaftsrechts.*

*An den Standorten Straßburg & Kehl verfügen wir über ein mehrsprachiges ca. 10-köpfiges Team mit Rechtsanwälten/-innen bzw. Avocats/Avocates, die in Deutschland und/oder Frankreich zugelassen sind.*

*Die Schwerpunkte unserer rechtlichen und strategischen Beratung liegen in den folgenden Bereichen:*

- ***Unternehmenskauf (M & A)***
- ***Corporate***
- ***Human Ressources***
- ***Compliance***
- ***International***
- ***Restructuring***
- ***Services & Products***
- ***Litigation***