



Die Bahnindustrie.

Verband der Bahnindustrie in Deutschland

Informationspapier

Umgang mit Maschinendaten

Überarbeitung der Version aus 12/2020
Update 10/2026

Inhalt

1	Die Definition von Maschinendaten	5
2	Rechtlicher Umgang mit Maschinendaten	6
2.1	Gesetzliche Rechtslage	6
2.1.1	Einordnung nach Sachen- und Immaterialgüterrecht	6
2.1.2	Einordnung nach Data Act	7
2.2	Möglichkeiten der vertraglichen Rechtsgestaltung	10
2.2.1	Interessenlage	11
2.2.2	Parteien einer vertraglichen Regelung	11
2.2.3	Form	12
2.2.4	Regelungsinhalte	12
2.2.5	Einschränkung der Vertragsfreiheit im Übrigen	13
2.2.6	Einschränkbarkeit der Pflichten zur Datenbereitstellung	13
2.2.7	Nicht dem Data Act unterliegende Maschinendaten	14
2.3	Abschließende Hinweise	14
2.4	Technische Gestaltung im Umgang mit Daten	15
2.5	Harmonisierung von Data Act und Cyber Resilience Act	15
	Abkürzungen	17
	Endnoten	18
	Impressum	19

Einleitung

Sehr geehrte Damen und Herren, liebe Kolleginnen und Kollegen,

in unserer zunehmend durch Digitalisierung und Automatisierung geprägten Zeit entstehen immer mehr Daten, die von Maschinen produziert werden und die zum Teil erheblichen Wert haben können und entsprechend sorgfältig behandelt und geschützt werden müssen. Aufgrund der nicht abschließend geklärten Rechtslage gibt es viele Unsicherheiten in Bezug auf Daten, Datenanalyse, Datenschnittstellen, Datenaustausch, Eigentum an und Schutz von Daten.

Diese Fachinformation hat zum Ziel, den Mitgliedsunternehmen des VDB in kompakter Form eine Einführung und Orientierung zum Umgang mit Maschinendaten zu geben. Sie hat infolge des Inkrafttretens der Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates (Data Act) eine Überarbeitung erfahren. Der Umgang mit Daten, die der Datenschutzgrundverordnung (DSGVO) unterfallen, ist zusätzlich entsprechend der DSGVO zu behandeln und wird hier nicht im Detail betrachtet. Die kontinuierliche Anpassung des Umgangs mit Daten an die weitere rechtliche und technische Entwicklung ist grundlegende Voraussetzung für verantwortungsvolles und rechtssicheres Handeln.

Für weitere Fragen stehen Ihnen die Geschäftsstelle des VDB und in den VDB-Mitgliedsunternehmen die Teilnehmer des Arbeitskreises Recht des VDB sehr gern zur Verfügung.

Wir wünschen eine angenehme Lektüre.

Wir weisen darauf hin, dass die Inhalte und Angaben dieses Leitfadens nach bestem Wissen sowie mit größtmöglicher Sorgfalt erstellt wurden. Der Herausgeber übernimmt keine Gewähr für die Richtigkeit, Vollständigkeit und Aktualität der bereitgestellten Inhalte und Informationen. Die Hinweise und Vorschläge geben die Meinung und Ansicht des Herausgebers wieder und genießen keinen Anspruch auf Richtigkeit. Dieser Leitfaden dient lediglich der Information und ersetzt daher keine fachliche oder anwaltliche Beratung im individuellen Umgang mit dem Thema Daten, so dass eine Verwendung, Nutzung oder Befolgung der dargestellten Hinweise und Vorschläge stets eigenverantwortlich und auf eigene Gefahr erfolgt.

Aus Gründen der besseren Lesbarkeit wird in diesem Text das generische Maskulinum verwendet. Alle personenbezogenen Bezeichnungen in diesem Text sind somit geschlechtsneutral zu verstehen.

1 Die Definition von Maschinendaten

Als **Maschinendaten** sollen für dieses Informationspapier solche Daten definiert werden, die ausschließlich von Sensoren, Maschinen und/oder Systemen erzeugt werden und keinen Personenbezug haben.

In der Bahnindustrie können verschiedene Arten von Maschinendaten vorhanden sein. Je nach Art und Herkunft können diese Maschinendaten in verschiedenen Formen vorliegen. Diese Daten können sowohl an oder in Schienenfahrzeugen als auch in der Bahninfrastruktur erzeugt werden. Die nachfolgende Tabelle zeigt ein paar Beispiele auf:

Arten von Maschinendaten	Beispiele
Betriebs- beziehungsweise Produktionsdaten	■ Not- und Gefahrenbedienungen ■ Geschwindigkeiten (von Schienenfahrzeugen) ■ Positionen (von Schienenfahrzeugen) ■ Fahrprofile (von Schienenfahrzeugen) ■ Stellzustände (von Weichen)
Diagnosedaten zur Nutzung durch den Betreiber/Eigentümer	■ Energieverbräuche (von Motoren) ■ Störungs- und Fehlermeldungen ■ Verschleißmeldungen ■ sicherheitsrelevante Fehlermeldungen ■ Wartungsfristüberwachung
Diagnosedaten zur Nutzung durch den Hersteller/Lieferanten	■ Detaillierte Diagnose- und Fehlerprotokolle, zum Beispiel Drehzahlen von Wellen ■ Temperaturen (von Schmiermitteln) ■ Schwingungen (von Wälzlagern) ■ Unrundheiten (von Rädern)
Systemdaten	■ Systemsoftware ■ systembezogene Projektierungen

Durch die Verarbeitung, Umwandlung, Analyse, Visualisierung, Interpretation oder sonstige Veränderung dieser Maschinendaten entstehen Informationen, die zum Beispiel für die Instandhaltungsplanung oder den Betrieb des Schienenverkehrs genutzt werden können. Dies können zum Beispiel die Restlebensdauer eines Radsatzlagers, die Verfügbarkeit von Güterwagen oder der Fahrtverlauf sein.

Werden Maschinendaten unter Zuhilfenahme weiterer Information ergänzt, können diese allerdings auch zu personenbezogenen Daten werden. Dies ist der Fall, wenn zum Beispiel über Schichtpläne oder mittels Benutzernamen in IT-Systemen Rückschlüsse auf einzelne Personen gezogen werden können – also zum Beispiel der gemessene Fahrverlauf einem einzelnen Lokführer zugeordnet werden kann. In diesem Fall müssten zudem die Vorgaben der DSGVO beachtet werden.

2 Rechtlicher Umgang mit Maschinendaten

2.1 Gesetzliche Rechtslage

Die Möglichkeit der wirtschaftlichen Nutzung von Maschinendaten richtet sich im Wesentlichen nach ihrer zivilrechtlichen Einordnung und, soweit Maschinendaten dem Data Act unterfallen, nach deren Regelungen.

Vorab ist darauf hinzuweisen, dass sich infolge des Data Act die Diskussion von einer gesetzlichen Verankerung des „Dateneigentums“ weg hin zur Normierung eines Anspruchs auf „Datenzugang“ entwickelt hat. Die Diskussion über die sachen- und immaterialgüterrechtliche Einordnung der Daten – als Vorfrage hinsichtlich eines Rechts an Daten – ist damit aktuell in den Hintergrund gerückt.

2.1.1 Einordnung nach Sachen- und Immaterialgüterrecht

Die vor Veröffentlichung des Data Act diskutierten Ansätze für eine sachen- und immaterialgüterrechtliche Einordnung von Daten haben bisher nicht zu einer einheitlichen Sichtweise hinsichtlich der Begründung eines „Rechts an Maschinendaten“ geführt.

Wegen fehlender Sachqualität [§ 90 BGB](#) kommen sowohl „Dateneigentum“ als auch „Datenbesitz“ als absolute Rechte nicht in Betracht.¹ Eine analoge Anwendung der Sacheigentumsvorschriften scheitert, denn Daten sind unbegrenzt reproduzierbar und ein nicht-rivalisierendes Gut. Sie können von mehreren Anwendern nebeneinander analysiert werden, ohne dass dieser Umstand zu einer Beeinträchtigung eines der Anwender führt.² Auch ist es nicht überzeugend, das Verwendungsrecht an Daten von der Eigentumszuordnung der erzeugenden Komponente abzuleiten, denn Daten sind weder „Früchte“ [§ 99 BGB](#) noch Gebrauchsvorteile [§ 100 BGB](#).³

Ein „Nutzungsrecht“ an einzelnen Maschinendaten über das Immaterialgüterrecht ist ebenfalls nicht möglich, da Maschinendaten keine persönliche geistige Schöpfung darstellen und somit kein Schutz als „Werk“ nach dem Urheberrechtsgesetz besteht.⁴ Urheberrechtsschutz kann jedoch dort greifen, wo durch schöpferische Verarbeitung der Maschinendaten Datensätze mit individuellem Charakter entstehen⁵. Der urheberrechtliche Leistungsschutz des Datenbankherstellers kann nicht einzelne Daten, sondern nur ihre Zusammenstellung in einer Datenbank schützen.⁶ Das Recht des Datenbankherstellers gilt allerdings nicht für Daten, die dem Data Act unterfallen [Artikel 43](#).⁷

Schließlich wird die Zuordnung von Maschinendaten zu einem Rechtssubjekt über analoge Anwendung der datenschutzrechtlichen Vorschriften abgelehnt.⁸

Maschinendaten können jedoch einem Schutz nach dem Gesetz zum Schutz von Geschäftsgeheimnissen unterliegen, sofern derjenige, der faktisch Zugriff hat, angemessene Geheimhaltungsmaßnahmen trifft. Danach wären unter anderem Ansprüche auf Unterlassung, Schadensersatz und Auskunft gegen unbefugten Zugriff denkbar.⁹

2.1.2 Einordnung nach Data Act

Maschinendaten können als „Daten“, „Produktdaten“ und/oder „verbundene Dienstdaten“ dem Data Act unterfallen.

2.1.2.1 Definitionen des Data Act

Von zentraler Bedeutung als Quelle für die dem Data Act unterfallenden Daten sind die Begriffe „vernetztes Produkt“ und „verbundener Dienst“.

Vernetztes Produkt

im Sinne des Data Act [Artikel 2 Ziffer 5](#) können in der Bahnindustrie beispielsweise verbaute Produkte mit Sensoren sein, die Informationen über das Produkt („**Produktdaten**“ im Sinne von [Artikel 2 Ziffer 15 Data Act](#)) erfassen und über eine Internetverbindung übermitteln.

Verbundener Dienst

kann in der Bahnindustrie beispielsweise in einem Fahrgastinformationssystem bestehen. Über den regulären Betrieb hinausgehende Dienste, wie zum Beispiel zusätzliche Beratungs- oder Analysedienstleistungen oder regelmäßige Reparatur- und Wartungsdienste, sollen allerdings keinen verbundenen Dienst im vorgenannten Sinne darstellen¹⁰.

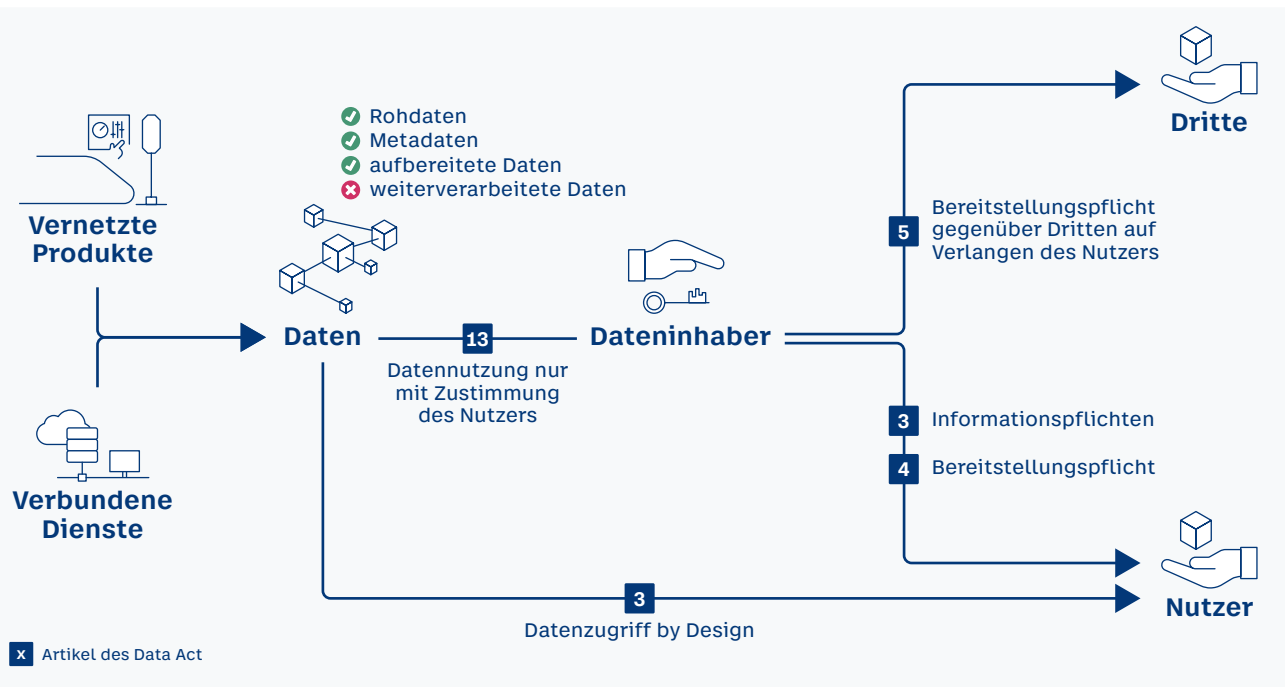
Durch „vernetzte Produkte“ und durch die Nutzung „verbundener Dienste“ können „**Produktdaten**“ oder „**verbundene Dienstdaten**“ [Artikel 2 Ziffer 16 Data Act](#) entstehen. Ob Maschinendaten „Daten“ im Sinne des Data Act sind und damit dessen Anwendungsbereich eröffnet ist, ist je nach **Grad ihrer Verarbeitung** zu beurteilen. Danach kommt folgende Einteilung in Betracht:¹¹

- **Rohdaten** (auch Quell- oder Primärdaten) sind Daten, die ohne jegliche weitere Form der Verarbeitung automatisch generiert werden. Exemplarisch kann es sich dabei um automatisch generierte Sensordaten handeln. Rohdaten unterfallen der Definition von „Daten“ im Sinne von [Artikel 2 Ziffer 1 Data Act](#).
- Rohdaten gleichgestellt sind Daten, die **vor der Weiterverarbeitung und Auswertung aufbereitet** werden, dies aber allein zu dem Zweck geschieht, die Daten dadurch überhaupt erst verständlich beziehungsweise für eine Vielzahl von Anwendungsfällen nutzbar zu machen. Beispiele hierfür sind Sensordaten, mittels derer eine physikalische Größe wie zum Beispiel Geschwindigkeit, Druck oder Temperatur angegeben wird. Auch diese Daten sollen dem Anwendungsbereich des Data Act unterfallen.¹²

- Anders ist es allerdings bei den **verarbeiteten Daten**. Sie unterfallen nicht dem Anwendungsbereich des Data Act. Kennzeichen verarbeiteter Daten ist, dass sie infolge mindestens eines Weiterverarbeitungsschrittes aus den vorgenannten Daten gefolgert oder abgeleitet werden. Dies gilt insbesondere für Ergebnisse, die sich lediglich aufgrund weiterer Investitionen – zum Beispiel mittels komplexer Algorithmen – erreichen lassen. Praktische Beispiele sind Analysedaten, wie Ausfallwahrscheinlichkeiten oder Verschleißdaten, die sich erst aufgrund des komplexen Zusammenspiels einer Vielzahl verschiedener Einzeldaten und unter Berücksichtigung statistischer Wahrscheinlichkeiten ermitteln lassen.

2.1.2.2 Akteure im Sinne des Data Act

Der Data Act differenziert die verschiedenen Akteure, die in Verbindung mit den Daten stehen oder ein Interesse an ihnen haben können.



Nutzer

ist im Sinne des [Artikel 2 Ziffer 12 Data Act](#) eine Person, die ein vernetztes Produkt besitzt oder der vertraglich zeitweilige Rechte für die Nutzung des vernetzten Produkts übertragen wurden oder die verbundenen Dienste in Anspruch nimmt. In der Bahnindustrie dürften das beispielsweise Eisenbahnverkehrsunternehmen sein, die eine digitalisierte Zugflotte betreiben. Ein vernetztes Produkt kann aber auch gleichzeitig mehrere Nutzer haben, beispielsweise einen Leasinggeber und ein Eisenbahnverkehrsunternehmen.

Dateninhaber

ist nach [Artikel 2 Ziffer 13 Data Act](#), wer die tatsächliche oder rechtlich vermittelte Verfügungsgewalt über die Daten ausübt.¹³ Dateninhaber können auch die Nutzer selbst sein. In der Bahnindustrie ist Dateninhaber beispielsweise ein Dienstleister für Diagnosedaten, je nach technischer Ausgestaltung aber auch der Hersteller oder sogar der Nutzer selbst.

Datenempfänger/Dritter

kann laut [Artikel 2 Ziffer 14 Data Act](#) jeder sein, der nicht Nutzer ist und entweder einen eigenen Anspruch auf Erhalt der Daten hat oder der diese auf Verlangen des Nutzers bereitgestellt bekommt. Eine zentrale Ausnahme hiervon besteht gemäß [Artikel 5 \(3\) Data Act](#) für sogenannte Gatekeeper im Sinne des [Artikel 3 der Verordnung \(EU\) 2022/1925 \(Gesetz über digitale Märkte – DMA\)](#). Ein Unternehmen, das hiernach als besonders einflussreicher Plattformdienst-Betreiber festgestellt wird, ist von der Möglichkeit des Datenempfangs ausgenommen und darf die Daten auch nicht verlangen – weder von einem Nutzer noch von einem Dateninhaber. Gleichzeitig dürfen an ihn auch von anderen Datenempfängern keine Daten weitergegeben werden.

2.1.2.3 Wesentliche Rechte und Pflichten

Der Data Act beinhaltet für die definierten Akteure eine Reihe von Rechten und Pflichten. Diese reichen von vorvertraglichen Informationspflichten bis hin zur Zugangsgewährung zu den Daten für Nutzer und Dritte.

Zunächst gilt für den Hersteller die Pflicht, vernetzte Produkte und verbundene Dienste **von Anfang an so zu konzipieren**, dass die Produktdaten für den Nutzer unkompliziert direkt zugänglich sind [Artikel 3 \(1\) Data Act](#). Dies meint insbesondere, dass die Daten für den Nutzer ohne Weiteres nutzbar sind, also vor allem in einem Format gefasst sind, welches ohne weiteren Aufwand weiterverwendet werden kann. Hieraus ergibt sich aber kein durchsetzbarer Anspruch für den Nutzer.¹⁴

Vor Vertragsschluss ist der Hersteller beziehungsweise Verkäufer dazu verpflichtet, dem Nutzer bereits ein Mindestmaß an Informationen im Hinblick auf die mit dem vernetzten Produkt oder dem verbundenen Dienst einhergehenden Daten bereitzustellen [Artikel 3 \(2\) Data Act](#).

Während der Abwicklung von Verträgen über vernetzte Produkte oder verbundene Dienste gewährt [Artikel 4 \(1\) Data Act](#) dem Nutzer einen unentgeltlichen Zugangsanspruch zu Daten im Sinne des Data Act, die beim Dateninhaber vorhanden sind. Eine – vertraglich zu regelnde – Einschränkung ergibt sich gemäß [Artikel 4 \(2\) Data Act](#) für die Beeinträchtigung besonders normierter Sicherheitsanforderungen mit schwerwiegenden nachteiligen Auswirkungen.

Ansprüche auf Zugangsgewährung während der Abwicklung können sich auch gegenüber Dritten ergeben, [Artikel 5 \(1\)](#) [Artikel 8 \(1\) Data Act](#). Ein solcher Anspruch hängt aber von einem darauf gerichteten Verlangen des Nutzers ab. Macht er dies geltend, entsteht für den Dateninhaber eine Pflicht zum Abschluss einer Vereinbarung mit dem Dritten über den Datenzugang. Der Dateninhaber kann in diesem Fall eine angemessene Gegenleistung verlangen¹⁵, die den Wert der Daten, den Aufwand der Bereitstellung sowie eine Marge enthalten kann [Artikel 9 \(1\)-\(3\) Data Act](#).¹⁶

Ab dem Zeitpunkt des Inverkehrbringens besteht für den Dateninhaber eine Obliegenheit zur Schaffung einer vertraglichen Grundlage, wenn er die erzeugten Daten nutzen möchte [Artikel 4 \(13\) Data Act](#).¹⁷

Einschränkungen und Ausnahmen zur Datenbereitstellung an den Nutzer oder einen Dritten

In jedem Fall der Datenbereitstellung oder -weitergabe verbietet der Data Act die Verwendung der Daten zur Entwicklung konkurrierender Produkte. Die Entwicklung neuer und innovativer Produkte ist weiterhin erlaubt [↗ Artikel 4 \(10\)](#) und [↗ Artikel 6 \(2\) e\) Data Act](#).

Im Hinblick auf sämtliche vorgenannten Rechte steht den Betroffenen – egal ob natürliche oder juristische Person – ein Recht auf Beschwerde bei der zuständigen Behörde zu [↗ Artikel 38 Data Act](#). Dies ist in Deutschland die Bundesnetzagentur [↗ Artikel 37 \(1\) Data Act](#), § 2 Absatz 1 DADG. Weiterhin besteht für alle Beteiligten die Möglichkeit, einen Verstoß gegen die Regelungen bei einer Streitbeilegungsstelle vorzubringen [↗ Artikel 4 \(9\)](#) [↗ Artikel 5 \(12\) Data Act](#).

Spannungsfeld zu Geschäftsgeheimnissen

Die Pflicht zur Bereitstellung der Daten nach [↗ Artikel 4](#) und [↗ Artikel 5 Data Act](#) kann mit dem Schutz von Geschäftsgeheimnissen nach [↗ § 2 Nummer 1 GeschGehG](#) kollidieren. Auch die dem Data Act unterfallenden Daten können zumindest dann Informationen von wirtschaftlichem Wert darstellen, wenn sie beispielsweise aufgrund ihres Detaillierungsgrades Rückschlüsse auf die Funktionsweise eines Produkts ermöglichen.¹⁸ Grundsätzlich besteht aber auch bei Geschäftsgeheimnissen die Pflicht zur Offenlegung der Daten. Allerdings ist dies mit Einschränkungen verbunden, die sich – abhängig davon, wem sie gegenüber bestehen – in ihrer Intensität unterscheiden. Hinsichtlich der hierfür bestehenden vertraglichen Gestaltungsmöglichkeiten wird auf das folgende [→ Kapitel 2.2](#) verwiesen.

2.2 Möglichkeiten der vertraglichen Rechtsgestaltung

Wie die vorangegangenen Ausführungen zeigen, ist die Möglichkeit der freien Verwendung von Maschinendaten, sofern sie dem Data Act unterfallen, eingeschränkt worden. Durch die Einführung des Data Act ist den Nutzern (zum Beispiel Betreibern von Fahrzeugen), wie auch Dritten (zum Beispiel Instandhaltern von Fahrzeugen) grundsätzlich ein Anspruch auf Zurverfügungstellung der Daten eingeräumt worden. Darüber hinaus benötigen die Dateninhaber (Fahrzeughersteller und Komponentenhersteller) gemäß Data Act nun die Zustimmung der Nutzer, um die von dem Fahrzeug beziehungsweise der Komponente generierten Daten zu erhalten [↗ Artikel 4 \(13\) Data Act](#).

Trotzdem ergeben sich Lösungsansätze für diese Situation aufgrund der Interessenlagen der Nutzer und der begrenzten, aber immer noch vorhandenen Einschränkungsmöglichkeiten der Zurverfügungstellung durch die Dateninhaber (Hersteller).

2.2.1 Interessenlage

Es ist davon auszugehen, dass die Nutzer von Fahrzeugen und Komponenten ein sachliches Interesse daran haben, dass die Hersteller beziehungsweise Dateninhaber die Maschinendaten trotz geänderter Rechtslage nutzen dürfen. Nur so können die Hersteller die Leistungen, Störungen oder Verfügbarkeiten ihres Produkts nachvollziehen und bewerten. Letztlich besteht auch ein begründetes Interesse der herstellerseitigen Sichtung von Daten zur Beobachtung der Produktsicherheit. Jene Daten können anschließend für die Erarbeitung von Empfehlungen für Optimierungen der Verfügbarkeit und Zuverlässigkeit der Produkte, der Senkung der Life-Cycle-Costs (LCC)- oder Instandhaltungskosten sowie der Verlängerung der Lebensdauer effektiv nutzbar gemacht werden. Die sich hieraus ergebenden technischen und vor allem wirtschaftlichen Vorteile für den Nutzer liegen auf der Hand. Insoweit kann es nur als sachgerecht im Interesse aller Beteiligten liegen, generierte Daten zu teilen.

Maßgeblich dürften hier die folgenden Interessen in Bezug auf die vernetzten Produkte beziehungsweise verbundenen Dienste sein:

- Interesse des Nutzers
 - für Zwecke des Betriebes
 - für Zwecke der Durchführung und Optimierung der Instandhaltung,
- Interesse des Herstellers und Instandhalters
 - zum Zwecke der Überwachung und Einhaltung der Produktsicherheit
- Interesse des Herstellers
 - an Optimierung und Produktverbesserung
 - zu Zwecken der Fehlererkennung und Mangelbehebung
- Interesse des Dritten, etwa in Person eines Instandhalters oder des Herstellers einer Komponente
- Interesse auf Wahrung der Geschäftsgeheimnisse einer Partei gemäß [↗ Artikel 4 \(6\) Data Act](#)

Die Berücksichtigung der genannten Interessen sollte den Ausgangspunkt für eine sachgerechte Regelung über Nutzungsmöglichkeiten an den Daten bilden. Aus diesem Grund empfiehlt es sich, insbesondere für den Dateninhaber, frühzeitig eine vertragliche Regelung mit dem Nutzer zu suchen.

2.2.2 Parteien einer vertraglichen Regelung

Als Parteien kommen hier die in [→ Kapitel 2.1.2.2](#) bezeichneten Akteure, namentlich der oder die Nutzer, der Dateninhaber und der Datenempfänger/Dritter in Betracht.

Hieraus kann sich angesichts der komplexen Vertragsgestaltung der rahmengebenden Dokumente und der eisenbahnrechtlichen Zuschreibung von Rollen in der Bahnbranche, etwa Fahrzeughalter oder ECM (Entity in Charge of Maintenance)-Verantwortliche Stelle, Klärungsbedarf ergeben. Deshalb kann es nahe liegen, dass die Parteien ihr Verständnis über ihre Rollen nach dem Data Act durch eine vertragliche Regelung niederlegen.

2.2.3 Form

Die Form der entsprechenden Vereinbarung dürfte vor allem durch die Form der Eingehung der der Datennutzung zugrundeliegenden Vereinbarung determiniert werden. Hier könnte man frühzeitig etwaig im Rahmen einer Vergabe vorgegebene Verträge entsprechend kommentieren oder im Rahmen von Verhandlungen auf interessengerechte Regelungen hinwirken.

Soweit die Abrede über Maschinendaten nicht bereits im Hauptvertrag, etwa einem Liefer- oder Instandhaltungsvertrag, abgebildet ist, empfiehlt sich bereits aus Transparenzgründen der Abschluss einer gesonderten Datennutzungsvereinbarung. Vorgaben aus dem Data Act hinsichtlich der Form der Regelung bestehen nicht.

2.2.4 Regelungsinhalte

2.2.4.1 Bestimmung der Maschinendaten

Bei Regelung der Datennutzung bietet es sich an, dass die Parteien sich zunächst darüber klar werden, ob Gegenstand der Vereinbarung nur Daten im Sinne des Data Act oder sämtliche Maschinendaten sein sollen. Daraufhin könnte der Umfang der von der Vereinbarung erfassten Daten definiert werden. Die nachstehenden Ausführungen kommen vor allem für die dem Data Act unterfallenden Daten zur Anwendung.

2.2.4.2 Art und Weise der Bereitstellung

Neben der Definition des Umfangs der Datenbereitstellung könnte auch die Art und Weise der Bereitstellung geregelt werden, um die Anforderungen des § 4 Absatz 1 Data Act umzusetzen. Essenziell dürfte die Definition der konkreten Umsetzung der Anforderungen des [Artikel 3 \(1\) Data Act](#) im zugrundeliegenden Sachverhalt sein, wie etwa die Bestimmung wann ein Datum als maschinenlesbar gilt. Hier empfiehlt sich die Fassung eines eigenen Leistungsverzeichnisses beziehungsweise einer eigenen technischen Spezifikation.

2.2.4.3 Bereitstellung an Dritte

Aufgrund des Rechts des Nutzers zur Bereitstellung der Maschinendaten an Dritte dürften die Parteien nach [Artikel 5 Data Act](#) Vereinbarungen über die Person des Dritten, Umfang, Dauer und Zweck der weiterzugebenden Maschinendaten und die Pflichten des Nutzers zur Wahrung von Geschäftsgeheimnissen beziehungsweise der Vertraulichkeit definieren, um einen schweren wirtschaftlichen Schaden für den Dateninhaber zu vermeiden. Dabei dürfte vor allem der Aspekt des Wettbewerbsschutzes fokussiert und sichergestellt werden, dass der Dritte entsprechend und unter Ausweisung der Mindestanforderungen des [Artikel 6 Data Act](#) verpflichtet wird.

2.2.4.4 Vergütung

Die Vereinbarung einer Vergütung für die Bereitstellung von Rohdaten und aufbereiteten Daten ist vom Data Act in der Regel nicht zugelassen, da diese als kostenlose Pflicht gestaltet ist.

Demgegenüber kann eine Vergütung vereinbart werden, wenn der Dateninhaber gemäß Vereinbarung mit dem Nutzer einem Dritten Daten direkt zur Verfügung zu stellen hat. In diesem Fall muss auch die Vergütungsregelung nach [Artikel 8 \(1\) Data Act](#) fair, angemessen, nicht-diskriminierend und transparent sein.

2.2.5 Einschränkung der Vertragsfreiheit im Übrigen

Die vorstehend beschriebene Vertragsgestaltung wird durch die gemäß Data Act vorgegebenen Umgehungsverbote eingeschränkt. Nach [Artikel 13 \(3\) Data Act](#) sind einseitig auferlegte Vertragsklauseln rechtsmissbräuchlich, wenn ihre Anwendung eine grobe Abweichung von der guten Geschäftspraxis bei Datenzugang und Datennutzung darstellt oder gegen das Gebot von Treu und Glauben verstößt. Beispielhafte Klauselverbote sind in [Artikel 13 \(4\) und \(5\) Data Act](#) benannt.

2.2.6 Einschränkung der Pflichten zur Datenbereitstellung

Im Rahmen der Vereinbarung sind Abstimmungserfordernisse zu erwarten. Zum Beispiel sind unterschiedliche Auffassungen zur Reichweite des unentgeltlichen Zugangsanspruchs des Nutzers nicht auszuschließen. Vor diesem Hintergrund ist zu prüfen, ob der Zugangsanspruch Grenzen findet.

Der Data Act selbst geht auf den Geheimnisschutz ein. Wie die Ausführungen zu den Interessenlagen der Akteure zeigen, kommt eine Kollision des Rechts zur Datenbereitstellung mit dem Recht zur Wahrung des Geheimnisschutzes in Betracht. Dies berücksichtigt der Data Act in den [Artikel 4 \(6\), \(7\)](#) sowie [Artikel 5 \(9\), \(10\)](#) explizit, wonach Geschäftsgeheimnisse zu wahren sind und eine Offenlegung nur insoweit erfolgen darf, als dies vom Vereinbarungszweck [Artikel 5 \(9\)](#) gedeckt ist und Vereinbarungen zum Schutz der Geschäftsgeheimnisse getroffen wurden [Artikel 4 \(6\)](#). Das umfasst auch Metadaten, die ebenfalls durch technische oder organisatorische Maßnahmen zu schützen sind.

Insbesondere in Bezug auf aufbereitete Daten dürfte jedoch ein Geheimhaltungsinteresse auch dort relevant werden, wo Sensordaten – etwa in Form von Energieverbrauchsdaten – Rückschlüsse auf die technische Ausgestaltung des Systems haben und die Preisgabe einen großen Schaden beim Dateninhaber verursachen könnten. Hier ist aber zu beachten, dass eine nicht von den Ausnahmen des [Artikel 5 \(9\)](#) beziehungsweise [Artikel 4 \(6\)](#) gedeckte Regelung zwischen Dateninhaber und Nutzer nach [Artikel 7 \(2\) Data Act](#) nicht bindend ist.

Sollte eine Vereinbarung nicht zustande kommen, ist der Dateninhaber berechtigt, die Weitergabe von Daten zu verweigern oder auszusetzen (Zugangsansprüche des Nutzers: [Artikel 4 \(7\)](#); des Dritten [Artikel 5 \(10\)](#)). Hierzu ist dann jedoch eine Mitteilung an die Behörde zu machen, die eine Beschreibung und Begründung der Nichtweitergabe enthalten muss.

In außergewöhnlichen Umständen ist der Dateninhaber selbst bei Zustandekommen einer Vereinbarung berechtigt, die Herausgabe zu verweigern [Artikel 4 \(8\)](#) und [5 Absatz \(11\) Data Act](#). Solche außergewöhnlichen Umstände wären aber nur dann anzunehmen, wenn trotz vor-

genannter Maßgaben kein hinreichender Schutz der Geheimnisdaten erreicht werden kann und infolge der Offenlegung mit hoher Wahrscheinlichkeit ein schwerer wirtschaftlicher Schaden zu befürchten ist. Darüber hinaus lässt Erwägungsgrund 31 Data Act erkennen, dass auch Auswirkungen auf Cyber Security und damit Produktsicherheitsaspekte Auslöser für außergewöhnliche Umstände sein können. Eine solche Ausnahme bedarf der hinreichenden und schriftlichen Begründung gegenüber dem Nutzer beziehungsweise dem Dritten sowie einer Mitteilung an die zuständige Behörde.

2.2.7 Nicht dem Data Act unterliegende Maschinendaten

Wie vorstehend etabliert unterfallen **weiterverarbeitete Daten** nicht dem Anwendungsbereich des Data Act. Weiterverarbeitete Daten sind aus Rohdaten oder aufbereiteten Daten abgeleitet und wenigstens einem weiteren Verarbeitungsschritt unterworfen. Das wäre zum Beispiel der Fall, wenn ein Instandhalter eine Software einsetzt, um aus Rohdaten zusätzliche Informationen zu gewinnen, die dann für Betriebs- oder Instandhaltungsempfehlungen (zum Beispiel im Zusammenhang mit Fahrerassistenzsystemen, Predictive Maintenance) genutzt werden können.

Zwar besteht mangels Anwendbarkeit des Data Act insoweit der Vorteil der Vertragsfreiheit der involvierten Akteure. Damit stellt sich wiederum – wie vor der Einführung des Data Act – die Frage der Zuordnung solcher Maschinendaten unter den beteiligten Akteuren. Dies lässt eine vertragliche Regelung als sinnvoll erscheinen. Hierin könnten die Parteien die örtlichen und zeitlichen Nutzungsrechte, deren Zweckbindung, eine etwaige Exklusivität, die Rechte zur Weitergabe an Dritte und schließlich Art und Umfang der Vergütung regeln.

Bei der vertraglichen Zuordnung der Rechte an Maschinendaten empfiehlt sich wieder die Orientierung an den Interessenlagen der Parteien (Hersteller, Betreiber, Instandhalter, Lieferanten und/oder Infrastrukturbetreiber, vergleiche oben → Kapitel 2.2.1). Als Indiz für die Zuordnung könnte zum Beispiel relevant sein, wer die Daten verarbeitet beziehungsweise das so erstellte Produkt entwickelt hat.

2.3 Abschließende Hinweise

Neben den vorgenannten Sachverhalten gibt es noch weitere Regelungskreise, wie zum Beispiel Haftung und Gewährleistung, Vertraulichkeit und IT-Sicherheit sowie Kostentragung oder gegebenenfalls Vergütung, welche die Parteien im Rahmen ihrer Vereinbarung adressieren sollten und regelsystematisch neben dem Data Act stehen. Da diese aber weitestgehend den allgemeinen zivilrechtlichen Grundsätzen entsprechen, wird auf eine vertiefte Betrachtung an dieser Stelle verzichtet.

Zur Erleichterung der vertraglichen Gestaltung hat die EU-Kommission entsprechend Artikel 41 Data Act  Mustervertragsklauseln veröffentlicht, die, wenn auch unverbindlich, gleichwohl hilfreich sein dürften.

2.4 Technische Gestaltung im Umgang mit Daten

Soweit ein Zugangsanspruch nach dem Data Act besteht, muss die Bereitstellung von Maschinendaten in standardisierten, dokumentierten, maschinenlesbaren Formaten erfolgen.¹⁹

In jedem Fall berücksichtigt der Data Act in [Artikel 11](#) geeignete technische Schutzmaßnahmen zum Schutz der Daten vor unbefugtem Zugang. Wie oben gezeigt, ist der Zugangsanspruch insbesondere in Fällen von Geschäftsgeheimnissen eingeschränkt.

Das Anliegen des Schutzes von Daten beziehungsweise den sie enthaltenden Systemen ist auch jenseits des Data Act relevant. Die gegenständlichen Systeme können einer sogenannten Kritischen Infrastruktur, genauer dem Sektor Transport und Verkehr²⁰ zuzuordnen sein. Durch die fortschreitende Verbreitung von Internet Protocol (IP)-basierten Systemen wächst auch die Gefahr des unerlaubten Zugriffs durch nicht autorisierte Personen. Daher ist, neben der Erzeugung und Weiterverarbeitung der Daten, ein besonderes Augenmerk auf den grundsätzlichen Schutz vor unberechtigtem Zugriff und die Veränderung der Daten durch Dritte zu legen (= Security). Um den Schutz der Systeme zu gewährleisten, sind die getroffenen/definierten Schutzmechanismen regelmäßig an die sich verändernde Bedrohungslage anzupassen. Als oberstes Ziel ist die Systemintegrität jederzeit zu gewährleisten, damit die Systeme, entsprechend ihrer Spezifikation, betrieben werden können (= Safety, beziehungsweise funktionale Sicherheit).

Auf Daten in Systemen (und deren Teilsystemen) in kritischen Anlagen des Sektors „Transport und Verkehr“ gemäß [§ 9 Absatz 3 BSI-KritisV](#) darf nicht unberechtigt zugegriffen werden. In diesen Systemen sind Zugriffs- und Nutzungsrechte auf der Basis der in den Systemen vorhandenen Rollen und Aufgaben (Segregation of Duties), das Prinzip der geringsten Rechte (Least Privilege), Multi-Factor-Authentication (MFA), Protokollierung, regelmäßige Rechte-Reviews sowie technische und organisatorische Maßnahmen zur Durchsetzung und Überwachung zu definieren, umzusetzen und dokumentiert gegenüber Aufsichtsbehörden und Auditoren nachweisbar zu halten.

2.5 Harmonisierung von Data Act und Cyber Resilience Act

Neben dem Data Act können auch andere EU-Digitalrechtsakte wie beispielsweise der Cyber Resilience Act („CRA“) auf dieselben Produkte anwendbar sein. So kann ein Produkt mit digitalen Elementen gemäß [Artikel 3 Ziffer 1 Cyberresilienz-Verordnung \(„PDE“\)](#) auch ein vernetztes Produkt oder eine damit verbundene Dienstleistung im Sinne des Data Act sein. So werden bestimmte vernetzte Hardware- und als auch Software-Produkte mit logischen oder physischen Schnittstellen zur Datenverbindung (CRA) auch Daten über ihre Nutzung sammeln und diese Produktdaten über das Internet kommunizieren (Data Act).

Das Wechselspiel zwischen CRA und Data Act wird durch die Kommission in ihrem rechtlich unverbindlichen „FAQ on the Cyber Resilience Act implementation“²¹ näher beleuchtet. Danach seien beide Rechtsakte ihrem Wesen nach ohnehin unterschiedlicher Natur und mithin einander ergänzend. Während erstere Anforderungen für die Bereitstellung von Produkten mit digitalen Elementen auf dem Markt festlegt, regelt letztere die Bereitstellung von Produktdaten und verbundener Dienstdaten an andere Unternehmen.

Sofern ein PDE gemäß des CRA auch den Vorgaben des Data Act unterliegt, Daten für Nutzer oder Dritte bereitzustellen  Artikel 4 (5) Data Act, ist es die Pflicht des Herstellers, sicherzustellen, dass die entsprechenden Anforderungen des Data Act ebenfalls als Teil der Risikobewertung im Sinne des CRA berücksichtigt werden. Hersteller sollten berücksichtigen, dass der Data Act den Zugang zu Produkt- und zugehörigen Dienstleistungsdaten für Nutzer und Dritte vorschreibt, aber auch Maßnahmen für Dateninhaber festlegt, um die Weitergabe von Daten in bestimmten Fällen zu beschränken oder zu verweigern²².

Der VDB hat seinen Mitgliedsunternehmen jüngst eigens für den CRA einen Leitfaden zur Verfügung gestellt, der aus dem Arbeitsausschuss Cyber- und Informationssicherheit (CIS) hervorgegangen ist.²³

Unklarheiten und Überschneidungen in den EU-Digitalregulierungen bedeuten große Belastungen für Unternehmen. Zur Optimierung der Anwendung der digitalen Regelwerke, darunter auch des Data Act und der DSGVO, hat die Europäische Kommission aus diesem Grund am 19. November 2025 eine Digital Omnibus-Verordnung²⁴ vorgeschlagen und ergänzend am 20. Januar 2026 ein neues Cybersicherheitspaket präsentiert, das darauf abzielt, die Cybersicherheitsresilienz und -fähigkeiten der EU zu aktualisieren und besser aufeinander abzustimmen.²⁵ Das Paket umfasst einen Vorschlag für eine überarbeitete Cybersicherheitsverordnung (CSA) und gezielte Änderungen der NIS2-Richtlinie. Der Vorschlag zielt darauf ab, Anforderungen und Verpflichtungen in einem Rechtsrahmen zu harmonisieren, der das Cybersicherheitsgesetz, die NIS2-Richtlinie, den CRA, die DSGVO sowie andere sektorspezifische Vorschriften umfasst.

Der VDB begrüßt die dringend angezeigten Bemühungen der EU um Vereinfachung des digitalen Regulierungsumfelds und wird diese Entwicklungen weiterhin mit Interesse begleiten.

Abkürzungen

Akronym	Erklärung
BGB	Bürgerliches Gesetzbuch
BSI	Bundesamt für Sicherheit in der Informationstechnik
CIS	Arbeitsausschuss Cyber- und Informationssicherheit
CRA	Cyber Resilience Act
CSA	Cybersicherheitsverordnung
DADG	Data Act-Durchführungsgesetz
DMA	Gesetz über digitale Märkte
DSGVO	Datenschutz-Grundverordnung
ECM	Entity in Charge of Maintenance
EU	Europäische Union
IP	Internet Protocol
KFZ	Kraftfahrzeug
KRITIS	Kritische Infrastrukturen
LCC	Life-Cycle-Costs
MFA	Multi-Factor-Authentication
NIS2	NIS2-Richtlinie
PDE	Produkt mit digitalen Elementen

Endnoten

- 1 MüKoBGB/Stresemann, 10. Aufl. 2025, BGB § 90 Rn. 25; Brandenburgisches Oberlandesgericht, Urteil v. 6.11.2019, 4 U 123/19; vergleiche auch OVG Koblenz v. 9.5.2025, 10 A 10446/24 Rn. 166 m. w. N.
- 2 Kolany-Raiser – Hoeren/Sieber/Holzner MMR-HdB, Werkstand: 63. EL Oktober 2025, Teil 15.1 Big Data im Multimediarrecht, Rn. 5
- 3 Kristl, MMR 2021, 386
- 4 Vgl. Prof. Dr. Jutta Stender-Vorwachs, LL. M. und Dipl.-Jur. Hans Steege in NJOZ 2018, 1361, 1362 „Wem gehören unsere Daten?“ m. w. N.
- 5 Reto Hilty, in: Rolf H. Weber/Reto M. Hilty (Hrsg.), Daten und Datenbanken, Zürich 1999, S. 86 f. (Datensätze); Philip Kübler, Rechtsschutz von Datenbanken (EU-USA-Schweiz), Diss., Zürich 1999, S. 49 f.; Wolfgang Straub, Softwareschutz, Zürich 2011, Rz. 56 (Datensätze).
- 6 Dreier/Schulze/Dreier, 8. Aufl. 2025, UrhG Vor § 87a Rn. 1.
- 7 Heinzke in: Czvchowski/Lettl/Steinrötter, Data Act, 1. Aufl. 2025, Artikel 43 Rn. 1, vergleiche aber ErwG 112 S. 2 der das Schutzrecht sui generis des Datenbankherstellers für nicht in den Anwendungsbereich des Data Act fallende Daten unberührt lässt.
- 8 Vgl. auch hier insoweit die Studie des Bundesministeriums für Verkehr und digitale Infrastruktur, „Eigentumsordnung“ für Mobilitätsdaten?, Berlin 2017, S. 47 f. m. w. N.
- 9 Zum Spannungsverhältnis zwischen Geheimnisschutz und Zugangsrechten unter dem Data Act unter → Kapitel 2.1.2
- 10 Siehe dazu Erwägungsgrund 17 Data Act.
- 11 Zur Differenzierung anhand von KFZ-Daten siehe Guidance on vehicle data, accompanying the Data Act | Shaping Europe's digital future Guidance on vehicle data, accompanying the Data Act | Shaping Europe's digital future der Europäischen Kommission.
- 12 Siehe dazu Erwägungsgrund 15 Data Act.
- 13 Haben mehrere Personen auf diese Weise Zugriff auf die Daten, kommen nach Dafürhalten der Europäische Kommission (FAQ Data Act Version 1.4 22.01.2026) auch mehrere Dateneinhaber in Betracht. Demgegenüber wird auch vertreten, dass nur der originäre Inhaber „Dateneinhaber“ sein kann (so etwa Lettl in: Czzychowski/Lettl/Steinrötter: Data Act, Artikel 2 Rn. 73).
- 14 So etwa Frank, Christian Dr. in: RlnPrax 2025, 51 Rn. 8, beck-online.
- 15 Dies gilt gegenüber eigenständig agierenden kleinen und mittleren Unternehmen gemäß der EU-Empfehlung 2003/361 sowie gemeinnützigen Forschungseinrichtungen nur eingeschränkt, Artikel 9 (4) Data Act.
- 16 Siehe dazu auch Erwägungsgründe 46 und 47 Data Act.
- 17 Siehe dazu im Detail unter Ziffer 2.2.
- 18 Kiefer/Schneider: Data Act und Geschäftsgeheimnisschutz in der Praxis (GRUR-Prax 2025, 648).
- 19 Artikel 33 Data Act
- 20 „KRITIS“ gemäß § 9 BSI-KritisV
- 21 digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-implementation-frequently-asked-questions
- 22 Zum Beispiel unter Verwendung der sogenannten „Handbremsen“ „Geschäftsgeheimnis“ und „Sicherheit“ (Data Act Artikel 4 (8), Artikel 5 (11) beziehungsweise Artikel 4 (2))
- 23 CRA Leitfaaden: Gesetz über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen
- 24 eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0837
- 25 digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act

Impressum

Herausgeber

© 10/2026

Verband der Bahnindustrie in Deutschland (VDB) e. V.

Universitätsstraße 2, 10117 Berlin

Lobyregister Nr. R003287

☎ +49 30 206289-0

✉ info@bahnindustrie.info

🏠 bahnindustrie.info

🏢 [Verband der Bahnindustrie in Deutschland \(VDB\) e.V.](http://Verband der Bahnindustrie in Deutschland (VDB) e.V.)
(German Railway Industry Association)

Bildnachweise

Titelbild: ©iStock

Abbildungen: ©webersupiran.berlin

Entwurf und Gestaltung

webersupiran.berlin

Der Verband der Bahnindustrie in Deutschland (VDB) e.V.

vertritt die Interessen von über 250 Unternehmen, von weltweit führenden Systemhäusern ebenso wie von spezialisierten mittelständischen „Hidden Champions“. Die Mitglieder des VDB entwickeln und fertigen Systeme und Komponenten für Schienenfahrzeuge und Infrastruktur mit rund 56.600 Mitarbeiterinnen und Mitarbeitern allein in Deutschland. Innovative Technologien „Made in Germany“ sorgen weltweit für exzellente Bahnsysteme, klimaschonende Mobilität und digitale Innovationen.

Die Bahnindustrie.

Verband der Bahnindustrie in Deutschland

bahnindustrie.info

