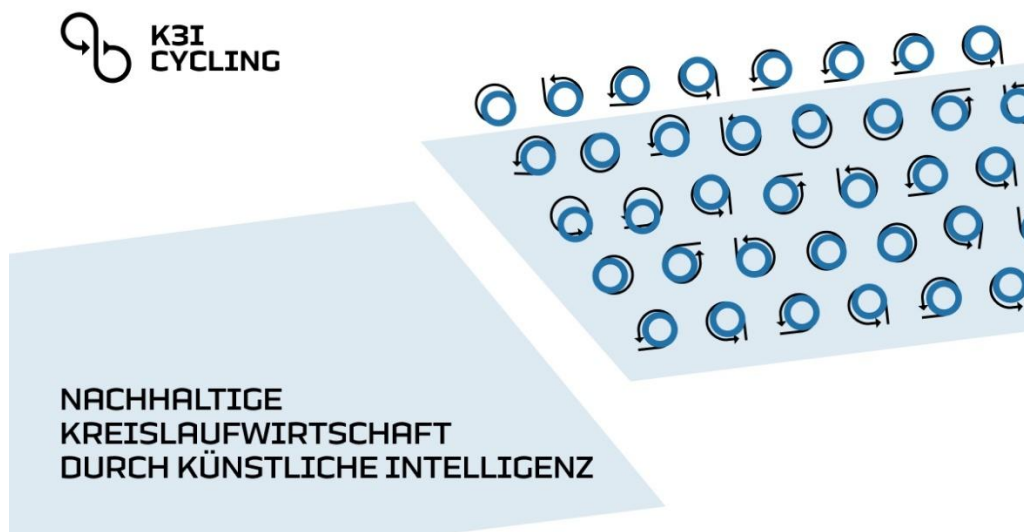




AP 8.1 Rechtliche Analyse und Begleitung

des Teilvorhabens

Rechtliche Analyse ausgewählter Aspekte der digitalisierten Kreislaufwirtschaft (FKZ: 033KI212)

im Vorhaben

KI-Anwendungshub Kunststoffverpackungen – Innovationslabor: K3I-Cycling – KI gestützte Optimierung der Kreislaufführung von Kunststoffverpackungen

August 2025¹,

Lehrstuhl für Rechtsinformatik,

Universität des Saarlandes

Bericht zur Einschätzung der rechtlichen Sachlage, inkl. Kurzbericht zu technischen Lösungsansätzen
Analyse der datenschutzrechtlichen Voraussetzungen für eine rechtskonforme Datenerfassung und -verarbeitung, insbes. unter Berücksichtigung von Social-Engineering Angriffen.

Analyse eines rechtlich zulässigen Datenaustauschs zwischen den einzelnen Projektpartnern unter Berücksichtigung des Schutzes von Geschäftsgeheimnissen.

Prüfung von Nutzungsrechten an entstehenden Produkten, insbes. ANTs

¹ Die Analyse ist bis August 2025 aktualisiert worden. Vereinzelt konnten spätere Aktualisierungen der Literatur noch berücksichtigt werden.

A. Datenverarbeitung bei der Abholung/dem Abtransport von Abfall

Damit sich die *Projektpartner bei K3I-Cycling* an die Vorgaben der DSGVO halten müssen, müsste zunächst deren (sachlicher) Anwendungsbereich eröffnet sein. Der sachliche Anwendungsbereich der Verordnung ist in Art. 2 DSGVO normiert und sieht vor, dass diese sowohl auf die automatisierte als auch nichtautomatisierte Verarbeitung **personenbezogener Daten** Anwendung finden soll, Abs. 1. Die Absätze 2 und 3 dieses Artikels legen fest, auf welche Verarbeitungsbereiche die DSGVO nicht angewendet wird.

I. Verarbeitung personenbezogener Daten

Vorab ist folglich zu klären, ob im projektrelevanten Szenario personenbezogene Daten verarbeitet werden. Fraglich ist, ob bei der Abbildung des Wertstoffkreislaufes mittels des ANTs auch Daten konkreter Haushalte einfließen können. Dies hängt von der Frage ab, welchen Prozess der ANT abbilden soll. Bildet der ANT den konkreten Prozess eines genau identifizierten Müllautos ab, können potenziell personenbezogene Daten erhoben werden. Eine Analyse dieses Szenarios erfolgt in den folgenden Abschnitten.

1. Begriffsbestimmung

Nach der Begriffsbestimmung in Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten alle Informationen, die sich auf eine **identifizierte** (d.h. konkret benannte) oder **identifizierbare Person** beziehen. Als bestimmbar wird eine natürliche Person angesehen, „die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind“². Die Definition wurde bewusst **weit** gefasst, um alle potenziellen Informationen über eine bestimmbare Person abzudecken und dieser ein angemessenes Schutzniveau garantieren zu können.³

Die Reichweite des Schutzes ist dabei nicht auf private oder sensible Informationen begrenzt, sondern umfasst grundsätzlich **jede Art von Informationen**, unter der Bedingung, dass es sich um Informationen über die betreffende Person handeln muss.⁴ Das ist dann der Fall, wenn die Information durch ihren Inhalt, aufgrund ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist.⁵

² Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, 4; COM (92) 422 final, S. 4.

³ Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, 4; COM (92) 422 final, S. 4 unter Verweis auf: Kommissionsmitteilung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und zur Informationssicherheit COM (90) 314 final, 13.9.1990, S. 19, Kommentar zu Art. 2.

⁴ Gola, in: Gola/Heckmann, DS-GVO – BDSG, 3. Aufl. 2022, DS-GVO Art. 4 Rn. 6.

⁵ EuGH, (2. Kammer), Urteil vom 20.12.2017 – C-434/16, NJW 2018, 767, 768 Rn. 35; Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, S. 10 f.

Eine natürliche Person ist dann im Sinne dieser Begriffsbestimmung **bestimmt**, wenn sie sich von anderen Personen einer Gruppe eindeutig unterscheiden lässt bzw. ist sie **bestimmbar**, wenn es eine Möglichkeit gibt, sie zu identifizieren.⁶ Für den Personenbezug eines Datums ist es nicht erforderlich, dass sich die Identität der Person direkt aus der Information selbst ergibt, vielmehr ist auch die **indirekte** Identifikation mithilfe weiterer Informationen ausreichend.⁷ Eine Person ist dann **identifizierbar**, wenn sie von dem Verantwortlichen ermittelt werden kann.⁸ In einem solchen Fall besteht der Personenbezug unabhängig davon weiter, ob eine Person namentlich benannt ist.⁹ Der Verantwortliche bestimmt die fragliche Person in der Regel mittels einer Verknüpfung mit weiteren Informationen.¹⁰ Das Verständnis des Begriffs „Identifizierbarkeit“ war bislang nicht ganz einheitlich; mittlerweile enthält Erwägungsgrund 26 zur DSGVO allerdings eine Auslegungshilfe. Um festzustellen, ob eine natürliche Person identifiziert werden kann, sind alle Mittel zu berücksichtigen, die von anderen Personen oder den Verantwortlichen **nach allgemeinem Ermessen wahrscheinlich** zur Identifizierung genutzt werden.¹¹ Dabei sind mittels einer Risikoprognose alle objektiven Faktoren wie Kosten, Zeitaufwand etc. heranzuziehen¹², wobei die zum Zeitpunkt der Verarbeitung¹³ einsetzbaren Technologien sowie technologische Entwicklungen Berücksichtigung finden müssen.¹⁴ Diesbezüglich muss zumindest ein **faktisches Risiko** der Herstellung eines Personenbezugs bestehen, welches dann abzulehnen ist, wenn die Identifizierung praktisch nicht durchführbar oder gesetzlich verboten wäre.¹⁵ Um eine solche Prognose treffen zu können, sind objektive Faktoren heranzuziehen. Hierzu gehört etwa die Frage, ob der Zweck der Verarbeitung bspw. aufgrund einer Nutzungssteigerung eine Identifizierung erforderlich macht oder ob der Identifizierung vertragliche oder organisatorische Hindernisse entgegenstehen, wie beispielsweise Vertragsstrafen.¹⁶ In einer abschließenden Abwägung ist der erwartete Kenntnisgewinn durch die Identifizierung dem vorangegangenen Aufwand gegenüberzustellen – das Ergebnis dieser Gegenüberstellung dürfte entscheidend für die Beurteilung des Personenbezugs von Daten sein.¹⁷

Fraglich ist, ob auch das **Zusatzwissen von Dritten** bei der Frage nach der Identifizierbarkeit Berücksichtigung finden muss.

⁶ Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, S. 14ff.

⁷ EuGH, Urteil vom 7.3.2024 – C-604/22, ZD 2024, 328, 330 Rn. 39; EuGH, Urteil vom 19.10.2016 – C-582/14, ZD 2017, 24, 25 Rn. 32; EuGH, Urteil vom 5.12.2023 – C-683/21, ZD 2024, 209, 212 Rn. 58.

⁸ Gola, in: Gola/Heckmann, DS-GVO Art. 4 Rn. 8.

⁹ Gola, in: Gola/Heckmann, DS-GVO Art. 4 Rn. 8.

¹⁰ Arning/Rothkegel, in: Taeger/Gabel, DS-GVO – BDSG – TDDDG, 5. Aufl. 2026, DS-GVO Art. 4 Rn. 30.

¹¹ Erwägungsgrund 26 S. 3 der DSGVO.

¹² Erwägungsgrund 26 S. 4 zur DSGVO.

¹³ Klar/Kühling, in: Kühling/Buchner, DS-GVO BDSG, 4. Auflage 2024, DS-GVO Art. 4 Nr. 1 Rn. 24; Arning/Rothkegel, in: Taeger/Gabel, DS-GVO Art. 4 Rn. 32.

¹⁴ Erwägungsgrund 26 S. 4 zur DSGVO.

¹⁵ EuGH, Urteil vom 19.10.2016 – C-582/14, ZD 2017, 24, 26 Rn. 46.

¹⁶ Arning/Rothkegel, in: Taeger/Gabel, DS-GVO Art. 4 Rn. 31.

¹⁷ Arning/Rothkegel, in: Taeger/Gabel, DS-GVO Art. 4 Rn. 31; EuG, Urteil vom 26.4.2023 – T-557/20, ZD 2023 399, 402 Rn. 103 ff.

Zu dieser Frage findet sich eine Ansicht¹⁸, die ein **absolutes Verständnis** des Personenbezugs zugrunde legt und davon ausgeht, dass im Sinne einer objektiven Betrachtungsweise jede potenzielle Möglichkeit zur Kenntnisnahme eines Dritten, auch eines rechtswidrigen Zugriffs auf die Daten beziehungsweise sogar das weltweite Wissen zu einer Identifizierbarkeit führt.¹⁹ Folglich wäre für die Frage nach der Identifizierbarkeit darauf abzustellen, ob **irgendein Dritter** die Person identifizieren kann.

Dieser Ansicht gegenüber steht eine Auffassung, die ein **relatives Verständnis** des Personenbezugs befürwortet. Danach soll im Wege einer subjektiven Betrachtungsweise nur auf die Möglichkeit zur Kenntnisnahme des jeweiligen Verantwortlichen abgestellt werden.²⁰

Das Wissen und die Mittel dritter Personen sind für die Frage des Personenbezugs dann einzubeziehen, wenn Daten an eine andere Person weitergegeben werden, die nach allgemeinem Ermessen wahrscheinlich in der Lage dazu ist, einen Personenbezug herzustellen, auch wenn die Daten für den Verantwortlichen selbst keinen Personenbezug aufweisen.²¹ Gleiches gilt, wenn Daten im Internet veröffentlicht werden.²²

In allen anderen Fällen kommt die **vermittelnde Ansicht**, die der EuGH im Breyer-Urteil entwickelt hat, zur Anwendung.²³ Im Einzelfall ist zu beurteilen, ob für den Verantwortlichen Mittel vorliegen, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, um eine Verknüpfung von Daten mit Zusatzinformationen, die einer anderen Person vorliegen, mit dem Ziel durchzuführen, die betroffene Person zu identifizieren.²⁴ Nach Ansicht des EuGH ist dies erfüllt, wenn der Verantwortliche über **rechtliche Mittel** verfügt, um sich die Daten des Dritten verfügbar zu machen, das heißt auf dessen Wissen und Mittel zugreifen kann.²⁵

Zu folgen ist der vermittelnden Ansicht des EuGH. Während die Ansicht zum absoluten Personenbezug zu weit geht und praktisch allen Daten Personenbezug bescheinigt, ist die relative Ansicht nicht mit einem umfassenden Schutz personenbezogener Daten und damit verbunden dem Persönlichkeitsrecht der Betroffenen vereinbar.

a) Projektbezogene Analyse

Fraglich ist, ob auch im konkreten Projekt ein Personenbezug angenommen werden kann. Es ist zumindest denkbar, dass die zu recycelnden und analysierenden Wertstoffe zu einzelnen Haushalten oder Personen zurückverfolgbar sind und Aufschlüsse über deren persönliches Abfall-Trennverhalten geben können. Bei den daraus resultierenden Informationen könnte es sich um personenbezogene Daten

¹⁸ Diese Ansicht wurde etwa durch die Artikel-29-Datenschutzgruppe vertreten, siehe hierzu etwa: Artikel-29-Datenschutzgruppe, Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten v. 27.02.2013, WP 202, S. 10.

¹⁹ Arning/Rothkegel, in: Taeger/Gabel, DS-GVO Art. 4 Rn. 33.

²⁰ Arning/Rothkegel, in: Taeger/Gabel, DS-GVO Art. 4 Rn. 34; Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017; Eßer in: Auernhammer DSGVO/BDSG – Kommentar, 8. Auflage 2023, Art. 4 DSGVO, Rn. 20.

²¹ Klar/Kühling, in: Kühling/Buchner, DS-GVO Art. 4 Nr. 1 Rn. 27.

²² Klar/Kühling, in: Kühling/Buchner, DS-GVO Art. 4 Nr. 1 Rn. 27.

²³ EuGH Urt. v. 19.10.2016 – Rs. C-582/14, NJW 2016, 3579 Rn. 49.

²⁴ Klar/Kühling, in: Kühling/Buchner, DS-GVO Art. 4 Nr. 1 Rn. 28.

²⁵ EuGH Urt. v. 19.10.2016 – Rs. C-582/14, NJW 2016, 3579 Rn. 49.

handeln. Informationen über das Abfall-Trennverhalten an sich stellen, wenn beispielsweise die Mülltonne direkt hinter dem Haus inspiziert und analysiert werden würde, grundsätzlich personenbezogene Daten dar. Im konkreten Projekt gelangen die Wertstoffe allerdings gesammelt in die Recycling-Anlage und müssten dort mühsam wieder getrennt werden, um eine Zurückverfolgung zu den einzelnen Haushalten zu ermöglichen. Auch erscheint problematisch, dass sich der Abfall unter Umständen nicht nur zu konkreten Einzelhaushalten zurückverfolgen lässt, sondern nur zu Mehrpersonenzusammenhängen, bei denen sich die Identifikation der einzelnen betroffenen Personen als schwierig erweisen dürfte.

In der Literatur findet sich hierzu auch der Hinweis, dass bspw. die Identifizierung eines Grundstückseigentümers anhand von Grundbuchdaten möglich ist, wenn dessen Entsorgungsverhalten von einem Entsorgungsunternehmen, welches Angaben zu Mülltonnen erfasst, überprüft wird.²⁶ Handelt es sich um ein gemietetes Objekt dürfte auch die Identifizierbarkeit der Mieter durch das Einwohnermeldeamt oder ggf. auch durch eine Abfrage beim Vermieter gegeben sein. Darüber hinaus könnte ein Personenbezug auch durch die Hinterlegung des Namens der jeweiligen Hauseigentümer beim örtlichen Entsorgungsunternehmen sowie anhand des Familiennamens der Hausbewohner durch die in der Regel am Hauseingang angebrachten Klingel- oder Briefkastenschilder hergestellt werden. Übertragen auf das Projekt K3I-Cycling, bei welchem auch das Recycling-Verhalten betrachtet werden soll, würde das bedeuten, dass die entsprechenden Daten einen Personenbezug aufweisen, da über die Grundbuch- beziehungsweise Hausverwaltungsdaten oder auch das Einwohnermeldeamt die Identität der einzelnen Personen ermittelt werden kann (folglich identifizierbar sind) und so Rückschlüsse auf deren Recycling-Verhalten gezogen werden können.

Bei **Personengruppen** ist ein Personenbezug zwar regelmäßig nicht mehr gegeben, wenn nur Sammelangaben über Personengruppen erfasst werden.²⁷ Es handelt sich allerdings dann um Einzelangaben mit Personenbezug zu einer Person, wenn über eine Personengruppe bestimmte Angaben gemacht werden, eine Einzelperson dabei als Gruppenmitglied gekennzeichnet wird **und** die fraglichen Angaben sich unmittelbar auf sie als Gruppenmitglied beziehen.²⁸ Dies ist auch dann der Fall, wenn die erhobenen Angaben zur Personengruppe statistische oder auf Durchschnittswerten beruhende Angaben sind.²⁹

Maßgeblich ist dabei jedoch die **Zweckbestimmung** der Information über die Personengruppe und ob die Gruppeninformation dem einzelnen Mitglied zugerechnet werden kann.³⁰ Zur Verdeutlichung kann folgendes Beispiel herangezogen werden: Erhält der Adressenbestand eines Stadtteils die zusätzliche Information, dass 90 Prozent der Bewohner eine bestimmte Partei gewählt haben, wird dadurch zwar die Einzelangabe festgehalten, dass der betroffene Bewohner zu einer so strukturierten

²⁶ Gola, in: Gola/Heckmann, DS-GVO Art. 4 Rn. 9.

²⁷ Gola, in: Gola/Heckmann, DS-GVO Art. 4 Rn. 12.

²⁸ Gola, in: Gola/Heckmann, DS-GVO Art. 4 Rn. 12.

²⁹ Gola, in: Gola/Heckmann, DS-GVO Art. 4 Rn. 12.

³⁰ Gola, in: Gola/Heckmann, DS-GVO Art. 4 Rn. 12.

Bevölkerungsgruppe gehört.³¹ Allerdings kann hieraus nicht automatisch der Schluss auf das vermutete Wahlverhalten des einzelnen Bewohners gezogen werden. Hierfür ist entscheidend, ob die Information über die Gruppe dem einzelnen Bewohner zuzurechnen ist. Relevant für die Bewertung der Zurechnung sind insbesondere die Informationsbewertung und -verwendung durch den Verantwortlichen.³²

Es ist allerdings davon auszugehen, dass regelmäßig der Aufwand zur Rückverfolgung zu einer konkreten Einzelperson oder Personengruppe **unverhältnismäßig** groß sein dürfte, zumindest sobald die Wertstoffe in die Recycling-Anlage gelangt sind. Denn zum einen werden dort zunächst die Umverpackungen entfernt, wodurch spätestens ab diesem Zeitpunkt aufgrund der anschließenden Durchmischung der einzelnen Bestandteile kaum eine Zuordnung zu einem bestimmten Abfallsack, geschweige denn einem konkreten Haushalt möglich sein dürfte. Um ab diesem Moment eine Rückverfolgung durchzuführen, müssten die einzelnen Wertstoffe vermutlich auf Fingerabdrücke oder DNA untersucht werden, um die dahinterstehende Person ermitteln zu können. Dies dürfte einen unverhältnismäßigen Aufwand darstellen.

Es sind allerdings auch Ausnahmefälle, sog. **Edge Cases**, denkbar, in denen eine Zurückverfolgung zu einer einzelnen konkreten Person sich wesentlich leichter gestalten könnte. Darunter würden beispielsweise Babynahrung, Windeln oder Medikamentendosen fallen, die dadurch konkret zugeordnet werden könnten, dass es beispielsweise im betreffenden Haus nur eine Einheit mit Baby/Kleinkind gibt oder nur eine Person, die verschreibungspflichtige Medikamente einnehmen muss. Ferner könnte auch das Gewicht des Abfalls eine Rolle spielen: So ist davon auszugehen, dass der Abfall einer Familie regelmäßig mehr als der eines Single-Haushaltes wiegt. In diesen Fällen dürfte der Aufwand zur Rückverfolgung zu einer konkreten Person nicht ganz so groß sein.

Anders zu bewerten könnte der Aufwand der Identifikation allerdings sein, wenn die Rückverfolgung zu einem früheren Zeitpunkt als der Verbringung in die Wertstoffanlage erfolgt. Bei Abholung des Abfalls ist die Rückverfolgung ohne unverhältnismäßig hohen Aufwand möglich.³³

Allerdings stellt sich in beiden beschriebenen Fällen die Frage, ob jeweils eine Datenverarbeitung im Sinne der DSGVO vorliegt. Von der Verordnung werden sowohl automatisierte als auch manuelle (nichtautomatisierte) Verarbeitungen erfasst.

Bei automatisierten Verarbeitungen werden automatisierte Mittel verwendet.³⁴ Unter automatisierten Mitteln dürften sämtliche heutzutage gebräuchliche rechnergestützte Verarbeitungen

³¹ Gola, in: Gola/Heckmann, DS-GVO Art. 4 Rn. 12.

³² Gola, in: Gola/Heckmann, DS-GVO Art. 4 Rn. 12.

³³ So wird etwa bei der Abholung des Hausmülls die Masse des Abfalls oft mit internen Wiegesystemen des Entsorgungsfahrzeugs bestimmt, vgl. etwa die seit dem 01.01.2011 standartmäßig durchgeführte Müllverwiegung des ZKE Saarbrücken, https://www.zke-sb.de/abfall/entsorgung/informationen_zur_muellverwiegung (zuletzt aufgerufen am 12.08.2025).

³⁴ Zerdick, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Aufl. 2024, DS-GVO Art. 2 Rn. 3.

personenbezogener Daten zu verstehen sein.³⁵ Aus Art. 2 Abs. 1 DSGVO geht hervor, dass nichtautomatisierte Verarbeitungen nur dann vom Anwendungsbereich der DSGVO erfasst sind, wenn die betreffenden personenbezogenen Daten in einem Datensystem gespeichert sind oder werden sollen. Zu klären ist, wann entlang der Wertschöpfungskette eine Datenverarbeitung in diesem Sinne vorgenommen wird. Hierbei sind verschiedene Zeitpunkte zu betrachten.

Die folgenden Überlegungen wurden zu einem früheren Zeitpunkt innerhalb des Projekts angestellt, in dem noch die Nutzung eines Chips zur Datenerfassung bei der Abfallsammlung in Betracht gezogen wurde.

Zunächst ist auf die Sammlung von Abfallsäcken abzustellen. Die reine Sammlung von Abfallsäcken durch die Leerung von Abfalltonnen ist nicht als Datenverarbeitung im Sinne der DSGVO anzusehen. Hinzutreten müssen weitere Handlungen, die eine Anwendung der DSGVO rechtfertigen. Eine Möglichkeit stellt das Abwiegen des abgeholten Abfalls dar. In verschiedenen Städten wird der Restmüll vor allem mit dem Ziel abgewogen, die Bürger zu einer konsequenten Mülltrennung anzuregen.³⁶ Des Weiteren ist auch der Einbau von Chips in Mülltonnen denkbar, um die Zuordnung zu bestimmten Grundstücken zu vereinfachen.³⁷ Werden entsprechende Mechanismen eingesetzt, ist eine Datenverarbeitung anzunehmen. Werden Chips mit einer eindeutigen Identifikationsnummer eingesetzt, so ist auch von der Verarbeitung personenbezogener Daten auszugehen. Auch im Falle des Abwiegens handelt es sich um die Verarbeitung personenbezogener Daten, da das Gewicht des Abfalls einem Haushalt zugeordnet werden kann. Durch die Verbindung zu einem Haushalt sind auch einzelne Personen identifizierbar. Diese Datenverarbeitungen sind aufgrund einer Rechtsgrundlage durchzuführen.

Art. 6 Abs. 1 lit. a bis f DSGVO normiert eine Reihe von Rechtsgrundlagen, die die Verarbeitung personenbezogener Daten ausnahmsweise erlauben.

Für den vorliegenden Fall relevant sind insbesondere die Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO, die Wahrnehmung von Aufgaben, die im öffentlichen Interesse liegen, nach Art. 6 Abs. 1 lit. e DSGVO sowie die Wahrung berechtigter Interessen nach Art. 6 Abs. 1 lit. f DSGVO.

*Die Einwilligung ist in Art. 4 Nr. 11 DSGVO legaldefiniert. Eine Einwilligung ist demnach jede von der betroffenen Person **freiwillig** für den bestimmten Fall in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Anforderungen an eine rechtskonforme Einwilligung ergeben sich aus Art. 7 DSGVO. Unter Einhaltung dieser Voraussetzungen kann eine Einwilligung Rechtsgrundlage für die Anbringung von Chips an Mülltonnen oder auch das Abwiegen des Abfalls dienen.*

³⁵ Zerdick, in: Ehmann/Selmayr, DS-GVO Art. 2 Rn. 3.

³⁶ In Saarbrücken wird der Abfall bspw. abgewogen: [Müllverwiegung | Zentraler Kommunalen Entsorgungsbetrieb](#).

³⁷ Die Stadt Löhne führte dies im Januar 2025 ein, [Ab November werden in Löhne die Mülltonnen ausgetauscht](#).

Als zweite potenzielle Rechtsgrundlage kommt Art. 6 Abs. 1 lit. e DSGVO in Betracht. Dieser erlaubt die Verarbeitung von Daten, soweit sie zur Wahrnehmung einer Aufgabe, welche im öffentlichen Interesse liegt, oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Der Erlaubnistatbestand nach Art. 6 Abs. 1 lit. e DSGVO ist auf behördliche oder staatlich veranlasste Verarbeitungsvorgänge zu begrenzen.³⁸ Zu beachten ist, dass Art. 6 Abs. 1 lit. e DSGVO nur in Verbindung mit einer weiteren Rechtsgrundlage, die sich entweder aus dem Unionsrecht oder aus dem Recht eines Mitgliedstaates ergibt, anwendbar ist. Dieser Umstand folgt aus Art. 6 Abs. 3 DSGVO. Mithin ist der eigentliche Erlaubnistatbestand nicht Art. 6 Abs. 1 lit. e DSGVO, sondern eine andere Norm aus dem Unions- oder mitgliedstaatlichen Recht. Nach dem jeweiligen Landesrecht sind öffentlich-rechtliche Entsorgungsträger zu Entsorgung bestimmter Abfälle verpflichtet. Privatpersonen sind zur Überlassung der Abfälle verpflichtet, § 17 Abs. 1 KrWG. Die Wahrnehmung einer öffentlichen Aufgabe ist mithin anzunehmen. Eine mit dieser öffentlichen Aufgabe verbundene Datenverarbeitung muss für einen legitimen Zweck erforderlich sein. Hierfür muss die Verarbeitung mit Art. 7 (Achtung des Privat- und Familienlebens) und 8 (Schutz personenbezogener Daten) GRCH zu vereinbaren sein.³⁹ Ferner sollte das vom Verantwortlichen angestrebte Ziel nicht anders als durch die Datenverarbeitung erreichbar, mithin erforderlich, sein.⁴⁰ Ziel des Einsatzes eines Wiegemechanismus ist die Reduktion von Abfällen und das Anhalten zu konsequenterer Mülltrennung. Mangels einer vergleichbaren Maßnahme kann das Abwiegen des Abfalls mithin auf Art. 6 Abs. 1 lit. e DSGVO in Verbindung mit der jeweiligen Landesvorschrift, die zur Entsorgung des Abfalls verpflichtet, herangezogen werden. Der Einsatz von Chips in Mülltonnen dient vor allem dem Ziel, die eindeutige Zuordnung einer Mülltonne zu einem Grundstück sicherzustellen sowie Fehlnutzungen und Doppelleerungen zu verhindern. Bei der Nutzung von Chips handelt es sich um eine effektive Maßnahme, um die beschriebenen Ziele umzusetzen. Allerdings bleibt darauf hinzuweisen, dass auf den Chips nur die nötigsten Daten gespeichert werden dürfen, mithin der Grundsatz der Datenminimierung eingehalten wird.⁴¹

Ferner kommt Art. 6 Abs. 1 lit. f DSGVO in Betracht. Auch berechnigte Interessen können die Verarbeitung personenbezogener Daten rechtfertigen, soweit nicht die Interessen und die Grundrechte und Grundfreiheiten der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, überwiegen. Nicht auf berechnigte Interessen berufen können sich indes Behörden und weitere Hoheitsträger, da die Rechtsgrundlage auf das Gleichordnungsverhältnis zwischen Privaten ausgelegt ist und nicht für das Verhältnis zwischen Hoheitsträgern und ihren Stellen als Verantwortliche und Privatpersonen als Betroffene.⁴² Diese Einschränkung besteht, um den Vorbehalt des Gesetzes hinsichtlich behördlichen Handelns nicht zu unterlaufen.⁴³ Die hier betrachtete Datenverarbeitung wird

³⁸ Buchner/Petri, in: Kühling/Buchner, DS-GVO Art. 6 Rn. 111; BVerwG, Urteil vom 27.03.2019 – 6 C 2/18, NJW 2019, 2556, 2561 Rn. 45.

³⁹ Buchner/Petri, in: Kühling/Buchner, DS-GVO Art. 6 Rn. 119.

⁴⁰ Reimer, in: Sydow/Marsch, DS-GVO BDSG, 3. Aufl. 2022, DSGVO Art. 6 Rn. 68.

⁴¹ Wie etwa in Löhne: Ab November werden in Löhne die Mülltonnen ausgetauscht.

⁴² Frenzel, in: Paal/Pauly, DSGVO BDSG, 4. Aufl. 2026, DSGVO Art. 6 Rn. 26.

⁴³ Dies folgt unter anderem aus Erwägungsgrund 47 S. 5 zur DSGVO.

durch öffentlich-rechtliche Entsorgungsträger durchgeführt. Mithin scheidet Art. 6 Abs. 1 lit. f. DSGVO als taugliche Rechtsgrundlage aus.

Nach der Sammlung von Abfallsäcken scheint eine Datenverarbeitung eher unwahrscheinlich. Abfallsäcke werden bereits im zum Abtransport genutzten Fahrzeug durchmischt, womit eine Zuordnung zu einer natürlichen Person mit einem unverhältnismäßig großen Aufwand verbunden wäre.

Die vorherigen Ausführungen greifen nur insoweit durch den ANT eine konkrete Situation eines bestimmten Abfallsammelfahrzeugs abgebildet wird.

II. Verantwortlichkeit im Sinne der DSGVO

Zu prüfen ist, welche Stakeholder entlang der Wertschöpfungskette aus datenschutzrechtlicher Sicht Verantwortlicher nach Art. 4 Nr. 7 DSGVO bzw. Auftragsverarbeiter nach Art. 4 Nr. 8 DSGVO ist. Mit der Eigenschaft als Verantwortlicher bzw. Auftragsverarbeiter gehen als Adressaten der DSGVO verschiedene Pflichten einher, wozu auch bspw. der Abschluss von Auftragsverarbeitungsverträgen oder im Falle einer gemeinsamen Verantwortlichkeit eines Joint Controller Vertrages, Art. 26, 28 DSGVO. Verantwortlicher ist nach Art. 4 Nr. 7 DSGVO, wer über die Zwecke und Mittel der Verarbeitung entscheidet, während Auftragsverarbeiter ist, wer die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet, Art. 4 Nr. 8 DSGVO.

Erfolgt eine Datenverarbeitung im Rahmen der Abholung von Abfallsäcken, so ist von der Verantwortlichkeit des öffentlich-rechtlichen Versorgungsträger auszugehen, welcher die Datenverarbeitung anordnet. Er bestimmt Zweck und Mittel der Verarbeitung. Wer die Datenverarbeitung letztlich durchführt, ist diesbezüglich irrelevant, da eine Auftragsverarbeitung angeordnet werden kann. Erforderlich ist in einem solchen Fall ein Auftragsverarbeitungsvertrag gemäß Art. 28 Abs. 3 DSGVO. Der notwendige Inhalt dieses Vertrages ergibt sich aus Art. 28 Abs. 3 S. 2 lit. a bis h DSGVO.

Da nicht davon auszugehen ist, dass außer dem öffentlich-rechtlichen Versorgungsunternehmen weitere Unternehmen entlang der Wertschöpfungskette personenbezogene Daten verarbeiten, stellt sich auch die Frage nach der Verantwortlichkeit im Sinne der DSGVO nicht.

B. Datenverarbeitung im/durch den ANT

Der ANT wird im Projekt in einer dezentralen Methode zur Prozessoptimierung eingesetzt und es wird nicht die Prozesskette beginnend beim Mülleinwurf betrachtet. Im Projekt ist allerdings geplant, den ANT dezentral zur Erfassung des Materialstroms anzuwenden. Hierbei wird die Prozesskette als neuronales Netz betrachtet und jeder Prozess bzw. jedes Unternehmen wird als Knoten des neuronalen Netzes betrachtet. Da der ANT insbesondere zur Betrachtung des Materialstroms eingesetzt wird und insbesondere technische Prozesse verbessern soll, ist nicht davon auszugehen, dass personenbezogene

Daten diesbezüglich anfallen. Fragen nach entsprechenden Rechtsgrundlagen und der Verantwortlichkeit im Sinne der DSGVO stellen sich daher nicht.

Zu betrachten sind jedoch auch diejenigen Regelungen, die nicht-personenbezogene Daten, wie etwa Maschinendaten, schützen. Der Data Act (DA) besitzt einen breiteren Anwendungsbereich als die DSGVO und erfasst neben personenbezogenen Daten auch nicht personenbezogene Daten, Art. 1 Abs. 2 DA, Art. 2 Nr. 4 DA. Hinsichtlich des Anwendungsbereichs der Verordnung gilt, dass der DA harmonisierte Vorschriften zu der Bereitstellung von Produktdaten und verbundenen Dienstdaten für den Nutzer des vernetzten Produkts oder verbundenen Dienstes (Art. 1 Abs. 1 lit. a DA) und zu der Bereitstellung von Daten durch Dateninhaber für Datenempfänger (Art. 1 Abs. 1 lit. b DA) umfasst.

Art. 2 DA enthält einige für den hiesigen Anwendungsfall relevante Legaldefinitionen.

- **Daten** sind nach Art. 2 Nr. 1 DA jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material.
- **Nicht-personenbezogene Daten** sind nach Art. 2 Nr. 4 DA Daten, die keine personenbezogenen Daten sind
- Ein **vernetztes Produkt** ist nach Art. 2 Nr. 5 DA ein Gegenstand, der Daten über seine Nutzung oder Umgebung erlangt, generiert oder erhebt und der Produktdaten über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang übermitteln kann und dessen Hauptfunktion nicht die Speicherung, Verarbeitung oder Übertragung von Daten im Namen einer anderen Partei – außer dem Nutzer – ist.
- **Nutzer** ist nach Art. 2 Nr. 12 DA eine natürliche oder juristische 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.
- **Dateninhaber** ist nach Art. 2 Nr. 13 DA eine natürliche oder juristische Person, die nach dieser Verordnung, nach geltendem Unionsrecht oder nach nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts berechtigt oder verpflichtet ist, Daten – soweit vertraglich vereinbart, auch Produktdaten oder verbundene Dienstdaten – zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat.
- **Datenempfänger** ist nach Art. 2 Nr. 14 DA eine natürliche oder juristische Person, die zu Zwecken innerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit handelt, ohne Nutzer eines vernetzten Produktes oder verbundenen Dienstes zu sein, und dem vom Dateninhaber Daten bereitgestellt werden, einschließlich eines Dritten, dem der Dateninhaber auf Verlangen des Nutzers oder im Einklang mit einer rechtlichen Verpflichtung aus anderem Unionsrecht oder aus nationalen Rechtsvorschriften, die im Einklang mit Unionsrecht erlassen wurden, Daten bereitstellt.

- **Produktdaten** sind nach Art. 2 Nr. 15 DA Daten, die durch die Nutzung eines vernetzten Produkts generiert werden und die der Hersteller so konzipiert hat, dass sie über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang von einem Nutzer, Dateninhaber oder Dritten – gegebenenfalls einschließlich des Herstellers – abgerufen werden können

Der ANT könnte ein vernetztes Produkt nach der Definition des DA sein bzw. aus mehreren vernetzten Produkten in diesem Sinne bestehen. Bei der geplanten Abbildung des Materialstroms werden einzelne Knoten des ANTs, die jeweils einen einzelnen Prozess abbilden sollen, verteilt eingesetzt. Die einzelnen ANT-Knoten können indes für sich genommen vernetzte Produkte darstellen. Bei der Nutzung des ANTs fallen verschiedene Daten an, wozu Materialdaten, Verarbeitungsdaten, Optimierungsdaten und Sensordaten gehören.⁴⁴

Materialdaten sind Informationen über die Produkte oder Materialien, die im realen Prozess verarbeitet werden; **Sensordaten** bezeichnen Daten, die durch am Prozess beteiligten Maschinen und Akteure über den laufenden Prozess und den Materialstrom mithilfe von verschiedenen Sensoren erhoben werden; **Verarbeitungsdaten** umfassen jene Informationen, die beteiligte Maschinen und Akteure benötigen, um ihren physischen Prozess virtuell im ANT abzubilden und die Verarbeitung somit virtuell zu simulieren. Zur Optimierung des Geschäftsprozesses wird der Einfluss jedes Prozessbeteiligten auf das Optimierungsziel berechnet und diese Informationen an die jeweiligen zutreffenden Prozessbeteiligten versendet – hierbei handelt es sich um **Optimierungsdaten**. Es fallen mithin nicht-personenbezogene Daten beim Einsatz des ANTs an, Art. 2 Nr. 4 DA.

Ferner ist es auch denkbar, dass bei der praktischen Umsetzung des ANTs Produktdaten nach Art. 2 Nr. 15 DA anfallen.

Für den Hersteller eines vernetzten Produktes fallen ebenso wie für den Inhaber von Daten, die durch ein vernetztes Produkt generiert werden, verschiedene Pflichten an, die sich aus dem DA ergeben.

I. Access-by-Design

Zunächst ist auf Art. 3 Abs. 1 DA hinzuweisen. Die Norm beinhaltet die Pflicht des Herstellers eines Produkts, dieses so zu konzipieren, dass die Produktdaten einschließlich der für die Auslegung und Nutzung dieser Daten erforderlichen relevanten Metadaten – standardmäßig für den Nutzer einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, direkt zugänglich sind. Es handelt sich bei Art. 3 Abs. 1 DA um Informationspflichten zugunsten der **Nutzer** im Sinne des Art. 2 Nr. 12 DA. Nutzer ist, wer ein vernetztes Produkt besitzt oder wem vertraglich zeitweilige Rechte für die Nutzung des vernetzten Produkts übertragen wurden. Fraglich ist, wer im Projektkontext **Nutzer** des ANTs und wer

⁴⁴ Siehe hierzu Abschnitt F zu den technischen Schutzmaßnahmen.

Dateninhaber ist. Dateninhaber ist, wer berechtigt oder verpflichtet ist, Daten – soweit vertraglich vereinbart, auch Produktdaten oder verbundene Dienstdaten – zu nutzen und bereitzustellen, die er während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat, Art. 2 Nr. 13 DA.

II. Datenzugangsrecht für Nutzer

Aus Art. 4 Abs. 1 DA folgt darüber hinaus ein Recht für den Nutzer eines Produkts oder eines verbundenen Dienstes auf den Zugang zu den erzeugten Daten.⁴⁵ Regelt werden der Zugang sowie die Nutzung von Daten durch den Nutzer. Der Dateninhaber ist dazu verpflichtet, dem Nutzer ohne Weiteres verfügbare Daten einschließlich der zur Auslegung und Nutzung der Daten erforderlichen Metadaten unverzüglich, einfach, sicher, unentgeltlich, in einem umfassenden, gängigen und maschinenlesbaren Format und – falls relevant und technisch durchführbar – in der gleichen Qualität wie für den Dateninhaber kontinuierlich und in Echtzeit bereitzustellen.

C. Dateneigentum

Eng verwandt mit der Frage der Einordnung als Nutzer, Dateninhaber oder Datenempfänger im Sinne des Data Acts ist die Frage nach dem Dateneigentum. Fraglich ist, ob der berechtigte Besitz an einem vernetzten Produkt (Nutzer) oder die berechtigte Nutzung oder Zurverfügungstellung von Daten (Dateninhaber) sich auch auf die Stellung als Eigentümer der Daten auswirkt. Der Eigentumsbegriff ist grundsätzlich mit dem Sachbegriff aus § 90 BGB verknüpft, wonach Sachen körperliche Gegenstände sind. Daten fallen nicht unter diesen Sachbegriff, weshalb auch der Eigentumsbegriff nicht ohne Weiteres auf Daten angewendet werden kann. Sind elektronische Informationen auf einem körperlichen Datenträger gespeichert, sind sowohl der Sach- als auch der Eigentumsbegriff auf den Datenträger anzuwenden.⁴⁶

Dies gilt allerdings nicht für die eigentlichen Daten, da diese unkörperlich sind. Dateneigentum in diesem Sinne gibt es nicht und das Konzept wird auch in der Literatur meist abgelehnt.⁴⁷ Häufig genutzt wird hingegen der Begriff der „Datenhoheit“, da auch bei Daten Nutzungskonflikte, etwa hinsichtlich des exklusiven Zugriffs auf bestimmte Daten, entstehen.⁴⁸ Allerdings wird auch in der Literatur teilweise damit argumentiert, dass es ein Irrglaube sei, dass gemeinsam generierte Daten eines vernetzten Produkts irgendetwem gehören müssten.⁴⁹ So hätten weder Produkthersteller, noch der Erzeuger der Daten Eigentum an diesen.⁵⁰

⁴⁵ Becker, IoT-Daten als Gemeineigentum – Der Data Act als digitale Utopie, RDi 2024, 615.

⁴⁶ Wagner, in: MüKo BGB, 9. Aufl. 2024, BGB § 823 Rn. 286.

⁴⁷ Veil, in: BeckOK DatenschutzR, 54. Edition, Stand 01.02.2025, DA Art. 1, Rn. 39 ff.; Wischmeyer/Herzog, Daten für alle? – Grundrechtliche Rahmenbedingungen für Datenzugangsrechte, NJW 2020, 288, 289; Specht-Riemenschneider, Der Entwurf des Data Act, MMR 2022, 809, 810, 818; Specht-Riemenschneider, Data Act – Auf dem (Holz-)Weg zu mehr Dateninnovation?, ZRP 2022, 137, 137 f..

⁴⁸ Martini/Kolain/Neumann/Rehorst/Wagner, Datenhoheit, MMR-Beilage 2021, 3, 5.

⁴⁹ Veil, in: BeckOK DatenschutzR, 54. Edition, Stand 01.02.2025, DA Art. 1, Rn. 39.

⁵⁰ Veil, in: BeckOK DatenschutzR, 54. Edition, Stand 01.02.2025, DA Art. 1, Rn. 39.

Diese Annahme ist allerdings nicht unumstritten. Teilweise wird auch vertreten, dass der Nutzer als Datenproduzent das immaterialgüterrechtliche Eigentum an verhaltensgenerierten Personendaten innehat.⁵¹ Dem widerspricht nunmehr ein Teil der Literatur, der das „Dateneigentum“ vielmehr an das wirtschaftlich verantwortliche Betreiben von vernetzten Produkten, die die Daten erzeugen, anknüpft.⁵² Teilweise wird auch diskutiert, die Zuordnung des „Eigentums“ an den Schaffensprozess (geistige oder technische Urheberschaft) der Daten anzuknüpfen.⁵³ Dieser Prozess der technischen Herstellung der Daten wird dabei als „Skripturakt“⁵⁴ bezeichnet.⁵⁵ Als originär Berechtigter (Skribent) wird nach dieser Ansicht derjenige angesehen, der durch Eingabe oder Ausführung eines Programms Daten selbst erstellt, mithin technischer „Ersteller“ der Daten ist.⁵⁶

Demgegenüber stehen Ansichten, die ein Ausschließlichkeitsrecht wie das Eigentum an Daten nicht anerkennen, sondern vielmehr ein Recht auf Geheimnisschutz einräumen.⁵⁷ Dies hängt insbesondere damit zusammen, dass der Geheimnisschutz kein Ausschließlichkeitsrecht einräumt, die Rechtsposition allerdings an ein mit dem Eigentum vergleichbares Ausschließlichkeitsrecht angenähert ist.⁵⁸ Teilweise werden auch Ansätze vertreten, die einen bloßen Datenbesitz statt eines Dateneigentums annehmen.⁵⁹ Mit dem Erlass des Data Acts wurde die Frage nach der Zuordnung von Daten zu einer bestimmten Person wieder neu diskutiert, was insbesondere damit zusammenhängt, dass der Data Act drei relevante Rollen (Dateninhaber, Datenempfänger, Datennutzer, Art. 2 Nr. 12, 13, 14 DA) definiert, die in einer bestimmten Beziehung zu Daten stehen.⁶⁰ Zu beachten ist, dass in den Definitionen keine Zuordnung im Sinne eines Eigentums an Daten vorgenommen wird. So ist der Nutzer eine natürliche oder juristische 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. Besitz an einem vernetzten Produkt sagt indes nichts über die Inhaberschaft an den darauf gespeicherten oder dadurch generierten Daten aus. Ähnlich verhält es sich mit der Definition des Dateninhabers, einer natürlichen oder juristischen Person, die dazu berechtigt oder verpflichtet ist Daten zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat. Die Berechtigung, Daten zu nutzen oder bereitzustellen, stellt ebenso kein Ausschließlichkeitsrecht in diesem Sinne dar. Trotzdem bleibt festzuhalten, dass Dateninhaber meist über eine De-Facto-

⁵¹ *Fezer*, Dateneigentum der Bürger, ZD 2017, 99, 100 f.

⁵² *Zech*, „Industrie 4.0“ – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151, 1159.

⁵³ *Hoeren*, Dateneigentum - Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486, 487.

⁵⁴ *Welp*, Datenveränderung (§ 303a StGB) – Teil 1, IuR 1988, 443, 447.

⁵⁵ *Hoeren*, Dateneigentum - Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486, 487; OLG Nürnberg, Beschluss vom 23.1.2013 - 1 Ws 445/12, ZD 2013, 282, 283.

⁵⁶ *Hoeren*, Dateneigentum - Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486, 487; *Welp*, Datenveränderung (§ 303a StGB) – Teil 1, IuR 1988, 443, 448.

⁵⁷ *Hoeren*, Alibaba und das Dateneigentum – 25 Jahre später, MMR 2023, 32, 33.

⁵⁸ *Hoeren*, Alibaba und das Dateneigentum – 25 Jahre später, MMR 2023, 32, 33.

⁵⁹ *Hoeren*, Datenbesitz statt Dateneigentum, MMR 2019, 5, 6.

⁶⁰ Zu den Definitionen eines früheren Entwurfs des DA: *Hoeren*, Alibaba und das Dateneigentum – 25 Jahre später, MMR 2023, 32, 33 ff.

Herrschaft über Daten und damit über eine eigentumsähnliche Position verfügen.⁶¹ Allerdings ist das Ziel des Data Act, diese Rechte zu begrenzen statt auszubauen.⁶²

Mithin ist festzuhalten, dass der Data Act kein Dateneigentum begründet.⁶³

Ferner besteht auch bei durch den ANT generierten Daten kein Eigentumsrecht.

Auch, wenn grundsätzlich davon auszugehen ist, dass kein Dateneigentum begründet werden kann, sind trotzdem die Rollen der Projektpartner im Szenario des ANT-Einsatzes zu bewerten. Da der ANT, oder die Verbindung aus ANT und Maschine, als vernetztes Produkt anzusehen ist, stellt sich die Frage, wer im Projektszenario als Dateninhaber und als Datennutzer anzusehen ist. Die Einordnung in diese Rollen ist relevant für mögliche aus dem DA folgende Ansprüche, wie etwa den Zugangsanspruch des Nutzers nach Art. 3 Abs. 1 DA. Es wird eine ANT-Schnittstelle geben, wobei Softwarepakete existieren, die dazu dienen, die Schnittstelle umzusetzen. Mithilfe der Softwarepakete können Maschinenhersteller die Schnittstelle an ihrer Maschine anbringen und verkaufen. Fraglich in diesem Szenario ist, ob die Maschinenhersteller als Dateninhaber angesehen werden können. Dies wäre dann der Fall, wenn sie dazu berechtigt oder verpflichtet wären, Daten – soweit vertraglich vereinbart, auch Produktdaten oder verbundene Dienstdaten – zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert haben. Es kommt mithin entscheidend darauf an, ob die Maschinenhersteller einen verbundenen Dienst erbringen. Hierfür stellt sich zunächst die Frage, ob das Softwarepaket des ANTs als verbundener Dienst im Sinne des DA anzusehen ist. Ein verbundener Dienst ist nach Art. 2 Nr. 6 DA ein digitaler Dienst, bei dem es sich nicht um einen elektronischen Kommunikationsdienst handelt, – einschließlich Software –, der zum Zeitpunkt des Kaufs, der Miete oder des Leasings so mit dem Produkt verbunden ist, dass das vernetzte Produkt ohne ihn eine oder mehrere seiner Funktionen nicht ausführen könnte oder der anschließend vom Hersteller oder einem Dritten mit dem Produkt verbunden wird, um die Funktionen des vernetzten Produkts zu ergänzen, zu aktualisieren oder anzupassen. Aus der Definition des verbundenen Dienstes geht indes hervor, dass ein vernetztes Produkt vorliegen muss, mit welchem der Dienst verbunden wird.

Die Maschinen, mit denen die ANT-Schnittstelle verbunden wird, sind nicht als Produkte im Sinne des DA anzusehen. Mithin mangelt es an der Voraussetzung, dass die ANT-Software mit einem vernetzten Produkt so verbunden werden muss, dass seine Funktionalitäten erreicht bzw. erweitert werden. Die ANT-Software trägt gerade nicht dazu bei, Funktionen der verbundenen Maschinen zu erreichen, die grundlegenden Funktionen der Maschine werden völlig unabhängig von der ANT-Software erbracht. Allerdings könnten die Funktionen der Maschine durch die ANT-Software als verbundener Dienst angepasst werden, soweit es zu einer Optimierung der Funktionen durch den ANT kommt. Jedoch ist auch dahingehend darauf hinzuweisen, dass die Maschinen, mit denen der ANT verbunden wird, nicht

⁶¹ Veil, in: BeckOK DatenschutzR, 54. Edition, Stand 01.02.2025, DA Art. 1, Rn. 43.

⁶² Veil, in: BeckOK DatenschutzR, 54. Edition, Stand 01.02.2025, DA Art. 1, Rn. 44.

⁶³ Veil, in: BeckOK DatenschutzR, 54. Edition, Stand 01.02.2025, DA Art. 1 Rn. 41.

als vernetzte Produkte in diesem Sinne anzusehen sind. Ein vernetztes Produkt entsteht erst bei der Verbindung von ANT und Maschine.

D. Datenaustausch zwischen den einzelnen Projektpartnern

Hinsichtlich des Datenaustausches zwischen den einzelnen Projektpartnern im Rahmen des Forschungsprojekts K3I-Cycling ist zu prüfen, ob dieser ebenfalls einer gesonderten rechtlichen Grundlage bedarf, sofern personenbezogene Daten (weiter-)verarbeitet werden oder eine solche „Weiterverarbeitung“ (Sekundärverarbeitung⁶⁴) von der ursprünglichen Verarbeitungsgrundlage gedeckt wird. Es ist folglich zu trennen zwischen den Konstellationen, in denen keine und in denen personenbezogene Daten verarbeitet werden.

I. (Weiter-)Verarbeitung/-leitung personenbezogener Daten

Vorab lässt sich festhalten, dass die DSGVO keinen besonderen Erlaubnistatbestand für die Verarbeitung von personenbezogenen Daten zu Forschungszwecken vorsieht, weswegen sich deren Rechtmäßigkeit nach den allgemeinen Vorschriften, Art. 5, 6 und 9 DSGVO richtet.⁶⁵ Hinsichtlich der Weitergabe personenbezogener Daten ist zu unterscheiden, ob es sich um Gesundheitsdaten iSv Art. 9 DSGVO handelt oder um nicht besonders sensible personenbezogene Daten, die den sonstigen Vorschriften und Anforderungen der DSGVO unterfallen.

Generell sieht die DSGVO für Forschung einige Ausnahmen und Privilegierungen vor: Zum Beispiel findet sich in Art. 5 Abs. 1 lit. b DSGVO eine Aufweichung des Zweckbindungsgrundsatzes, wonach, unter Beachtung des Art. 89 Abs. 2 DSGVO, Daten für Forschungszwecke unter festgelegten Bedingungen privilegiert weitergenutzt werden können.⁶⁶ Weitere Ausnahmen finden sich etwa in Art. 5 Abs. 1 lit. e (Speicherbegrenzung), in Art. 9 Abs. 2 lit. j (Verbot der Verarbeitung besonders sensibler Daten), in Art. 14 Abs. 5 lit. b (Einschränkung der Informationspflicht) und in Art. 17 Abs. 3 lit. d DSGVO (Löschpflicht).⁶⁷

⁶⁴ Unter dem Begriff der Sekundärverarbeitung wird die Weiterverarbeitung personenbezogener Daten verstanden, die zuvor zu anderen Forschungszwecken oder nicht-forschungsbezogenen Zwecken verarbeitet wurden, verstanden, *Bronner/Wiedemann*, Rechtmäßigkeit der Datenverarbeitung bei wissenschaftlicher Forschung an staatlichen Hochschulen, ZD 2023, 77, 79.

⁶⁵ Das nationale Datenschutzrecht sieht hierbei jedoch teilweise abweichende Regelungen vor; vgl. etwa § 27 Abs. 1 S. 1 BDSG, wonach eine Datenverarbeitung auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig sein kann, sofern die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen.

⁶⁶ *Weichert*, Die Forschungsprivilegierung in der DS-GVO, ZD 2020, 18, 19; *Rossnagel*, Datenschutz in der Forschung, ZD 2019, 157, 159.

⁶⁷ *Rossnagel*, Datenschutz in der Forschung, ZD 2019, 157, 159.

1. Begriff der Forschung

Der Begriff der „Forschung“ wird in der DSGVO nicht eigens definiert. Erwägungsgrund 159 S. 2 zur DSGVO enthält eine Form der Interpretationshilfe, wonach wissenschaftliche Forschungszwecke im Sinne der DSGVO weit auszulegen sind und umfassen die Verarbeitung für beispielsweise die technologische Forschung und die privat finanzierte Forschung.⁶⁸ Auch die Forschung mit Big-Data-Anwendungen soll von diesem weiten Verständnis des Forschungsbegriffs umfasst sein.⁶⁹

a) *Verarbeitung sonstiger personenbezogener Daten*

Bezüglich der Verarbeitung sonstiger personenbezogener Daten ist danach zu unterteilen, ob für deren Weitergabe eine Einwilligung erteilt wurde oder eine Sekundärnutzung ohne Einwilligung erfolgt.

aa) Weitergabe mit Einwilligung

Wie schon die (erstmalige) Verarbeitung kann auch die Weitergabe personenbezogener Daten aufgrund einer diesbezüglich erteilten Einwilligung iSv Art. 6 Abs. 1 S. 1 lit. a DSGVO erfolgen. Dabei gelten die allgemeinen Voraussetzungen aus Art. 4 Nr. 11, 7 DSGVO, sodass die Einwilligung insbesondere freiwillig, informiert und unmissverständlich erteilt werden muss.⁷⁰ Dementsprechend müsste die betroffene Person bereits vor Erhebung der Daten über die angestrebte Weitergabe der Daten hinreichend informiert werden.⁷¹ Die Einwilligung muss überdies grundsätzlich für die jeweilige konkrete Datenverarbeitung erteilt werden.⁷² Diesbezüglich wurde aber bereits vom Richtliniengeber berücksichtigt, dass im Rahmen von Forschungsvorhaben zum Zeitpunkt der Erhebung der Daten das spätere Vorhaben noch nicht in Gänze abzusehen sein kann. Daher finden sich in Erwägungsgrund 33 Ausführungen dazu, dass im Rahmen wissenschaftlicher Forschung weniger strenge Anforderungen an die Bestimmtheit der Einwilligung zu stellen sind.⁷³ Bislang ist jedoch noch nicht abschließend geklärt, wie eine solche weniger bestimmte Einwilligung aussehen könnte und von den Verantwortlichen auszugestalten wäre.⁷⁴ Auf europäischer Ebene ist in dem Data Governance Act (DGA) die Möglichkeit des Einsatzes standardisierter Einwilligungsformulare zur Erklärung eines „broad consent“ vorgesehen, Art. 25 DGA (Data-Governance-Act).⁷⁵ Auch Konzepte dynamischer oder mehrstufiger Einwilligung

⁶⁸ Golla, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Aufl. 2019, § 23 Rn. 14.

⁶⁹ Herbst, in: Auernhammer, BDSG § 27 Rn. 10; Keßler, Intelligente Roboter - neue Technologien im Einsatz, MMR 2017, 589, 591; Paal/Hennemann, Big Data im Recht, NJW 2017, 1697, 1700.

⁷⁰ Specht-Riemenschneider/Wehde, Forschungsdatenzugang, ZGI 2022, 3, 5.

⁷¹ Specht-Riemenschneider/Wehde, Forschungsdatenzugang, ZGI 2022, 3, 5.

⁷² Stemmer in: BeckOK Datenschutzrecht, 54. Ed. 01.11.2025, DS-GVO Art. 7 Rn. 77.

⁷³ Lauber-Rönsberg, in: Putnings/Neuroth/Neumann, Praxishandbuch Forschungsdatenmanagement, 2021, S. 104; Stemmer, in: BeckOK Datenschutzrecht, 54. Ed. 01.11.2025, DS-GVO Art. 7 Rn. 81.

⁷⁴ Die Medizininformatikinitiative hat für die medizinische Forschung einen Mustertext für die breite Einwilligung in die Sekundärnutzung pseudonymisierter Daten entwickelt, Specht-Riemenschneider/Wehde, Forschungsdatenzugang, ZGI 2022, 3 (5); <https://www.medizininformatik-initiative.de/de/mustertext-zur-patienteneinwilligung>, abgerufen am 01.08.2025.

⁷⁵ Data Governance Act v. 30.5.2022, VO (EU) 2022/868, abrufbar unter: <https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng>

sind möglich und denkbar.⁷⁶ Mit den reduzierten Anforderungen an die Einwilligung darf jedoch nur dann gearbeitet werden, wenn eine vollständige Zweckangabe bis zum Zeitpunkt der Datenerhebung schlechthin ausgeschlossen ist.⁷⁷ Dann muss jedoch zumindest eine möglichst präzise und nachvollziehbare Eingrenzung des Forschungsvorhaben erfolgen und es müssen ergänzend Maßnahmen zur Kompensation ergriffen werden, die der Herstellung von Transparenz, Vertrauen und Datensicherheit dienen.⁷⁸

Im Projekt dürfte sich jedoch die Einholung einer Einwilligung der betroffenen Personen in Gestalt der Wertstoffentsorgers schwierig gestalten beziehungsweise für die Verantwortlichen einen unverhältnismäßigen Aufwand mit sich bringen.

bb) Sekundärnutzung ohne Einwilligung

Die Weitergabe von Daten innerhalb des Projekts muss jedoch nicht zwangsläufig auf eine Einwilligung gestützt werden, da auch andere *Rechtmäßigkeitstatbestände* in Betracht kommen.

i) Datenverarbeitung zur Aufgabenwahrnehmung im öffentlichen Interesse

In Betracht kommen dabei insbesondere Art. 6 Abs. 1 S. 1 lit. e und f DSGVO. Dabei kann **Art. 6 Abs. 1 S. 1 lit. e DSGVO** ausschließlich zur Rechtfertigung von Datenverarbeitungen durch öffentliche Stellen dienen.⁷⁹ Es ist jedoch erforderlich, dass dem jeweiligen Verantwortlichen die Datenverarbeitung zur Wahrnehmung seiner Aufgabe übertragen wurde. Eine solche Aufgabenzuweisung erfolgt durch rechtliche Vorgaben der Mitgliedsstaaten oder der Union, weswegen lit. 3 nicht als für sich alleinstehender Erlaubnistatbestand verstanden werden kann.⁸⁰ Der Norm liegt ein streng funktionaler Ansatz zugrunde.⁸¹ Über sie lässt sich insbesondere die Datenverarbeitung zu Forschungszwecken durch Universitäten als öffentlich-rechtliche Forschungseinrichtungen rechtfertigen, da für diese durch die Hochschulgesetze der Länder explizit eine Zuweisung von Forschungsaufgaben erfolgt.⁸²

Sofern die Verarbeitungen zu wissenschaftlichen Forschungszwecken erfolgt, hat der Verantwortliche nach Art. 89 Abs. 1, 2 DSGVO geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen zu ergreifen. Art. 89 Abs. 1 DSGVO listet diesbezüglich explizit den Grundsatz der Datenminimierung und insoweit von Relevanz die Pseudonymisierung auf.

Vorschlag der EU-Kommission v. 25.11.2020 für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Data Governance Act), abrufbar unter: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767>.

⁷⁶ Specht-Riemenschneider/Wehde, Forschungsdatenzugang, ZGI 2022, 3, 6.

⁷⁷ Bronner/Wiedemann, Rechtmäßigkeit der Datenverarbeitung zu wissenschaftlicher Forschung an staatlichen Hochschulen, ZD 2023, 77, 79.

⁷⁸ Bronner/Wiedemann, Rechtmäßigkeit der Datenverarbeitung zu wissenschaftlicher Forschung an staatlichen Hochschulen, ZD 2023, 77, 79f.; Datenschutzkonferenz (DSK), Beschluss zur Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ im Erwägungsgrund 33 der DS-GVO, v. 03.04.2019.

⁷⁹ Specht-Riemenschneider/Wehde, Forschungsdatenzugang, ZGI 2022, 3, 6.

⁸⁰ Taeger in: Taeger/Gabel, DSGVO Art. 6 Rn. 116.

⁸¹ Albers/Veit in: BeckOK Datenschutzrecht, 54. Ed. 01.08.2025, DS-GVO Art. 6 Rn. 56; Taeger, in: Taeger/Gabel, DSGVO Art. 6 Rn. 124.

⁸² Golla in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 23 Rn. 43.

Zwar gibt es im Projekt einige Projektpartner, die an den Universitäten angesiedelt sind (z.B. der Lehrstuhl für Rechtsinformatik an der Universität des Saarlandes), es gibt aber auch eine Vielzahl von Projektpartnern, die nicht als öffentlich-rechtliche Forschungseinrichtungen einzuordnen sind und sich dementsprechend nicht auf Art. 6 Abs. 1 S. 1 lit. e DSGVO berufen könnten.

ii) Datenverarbeitung aufgrund eines berechtigten Interesses

Eine Datenverarbeitung zu wissenschaftlichen Zwecken, wie sie im Rahmen des Projekts erfolgen würde, könnte jedoch auf **Art. 6 Abs. 1 S. 1 lit. f DSGVO** gestützt werden. Diese Vorschrift verlangt eine Interessensabwägung zwischen den berechtigten Interessen des Verantwortlichen oder eines Dritten und den Interessen oder Grundrechten der betroffenen Personen, wobei jeweils die Umstände des Einzelfalls zu berücksichtigen sind.⁸³ Die Verarbeitung darf beim Vorliegen einer Gleichrangigkeit der Interessen durchgeführt werden.⁸⁴ Als berechtigtes Interesse eines Verantwortlichen kann auch das Forschungsinteresse angesehen werden.⁸⁵

Auf Art. 6 Abs. 1 S. 1 lit. f DSGVO können sich jedoch grundsätzlich nur private Beteiligte berufen, da es Behörden nach Art. 6 Abs. 2 DSGVO verwehrt ist, sich auf Art. 6 Abs. 1 S. 1 lit. f zu berufen. Diese können sich allerdings wiederum auf Art. 6 Abs. 1 S. 2 lit. e DSGVO stützen.

Wann ein Überwiegen des Forschungsinteresses anzunehmen ist, ist noch nicht abschließend geklärt.

1. Landesrechtliche Erlaubnistatbestände

Da die Projektbeteiligten bei K3I-Cycling in verschiedenen Bundesländern angesiedelt sind, können auch landesrechtliche Erlaubnistatbestände eine Rolle spielen.⁸⁶

2. Zweckänderung nach Art. 6 Abs. 4 DSGVO

Eine Weitergabe und daran anschließende Verarbeitung der Daten zu anderen Zwecken könnte auch nach Art. 6 Abs. 4 DSGVO möglich sein. Sofern die Daten nach der Zweckänderung zu wissenschaftlichen oder historischen Forschungszwecken verarbeitet werden sollen, wird von der Vereinbarkeit der Sekundärnutzung mit dem Ursprungszweck der Verarbeitung ausgegangen, Art. 5 Abs. 1 lit. b DSGVO.⁸⁷ Die weiteren Anforderungen des Art. 6 Abs. 4 DSGVO sind in dieser besonderen Konstellation dann nicht mehr zu berücksichtigen, denn die Vereinbarkeit wird von Art. 5 Abs. 1 lit. b

⁸³ Taeger in: Taeger/Gabel, DSGVO Art. 6. Rn. 172.

⁸⁴ Schulz, in: Gola/Heckmann, DS-GVO Art. 6 Rn. 62; Specht, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 9 Rn. 50.

⁸⁵ Specht-Riemenschneider/Wehde, Forschungsdatenzugang, ZGI 2022, 3 (6).

⁸⁶ Im Saarland bspw. § 23 SaarIDSG.

⁸⁷ Specht-Riemenschneider/Wehde, Forschungsdatenzugang, ZGI 2022, 3, 7.

DSGVO fingiert.⁸⁸ Zu berücksichtigen sind dabei allerdings die in Art. 89 Abs. 1 DSGVO aufgelisteten Voraussetzungen, wonach insbesondere technische und organisatorische Maßnahmen ergriffen werden müssen, mit denen unter anderem auch der Grundsatz der Datenminimierung gewährleistet wird.⁸⁹ Diese Privilegierung in Bezug auf den Grundsatz der Zweckbindung geht jedoch nicht einher mit einer Befreiung vom Grundsatz des Erfordernisses der Rechtmäßigkeit der Datenverarbeitung, Art. 5 Abs. 1 lit. a DSGVO.⁹⁰ Es bedarf folglich, neben der fingierten Vereinbarkeit der Verarbeitungszwecke, weiterhin einer eigenständigen Rechtsgrundlage für die Weiterverarbeitung der Daten nach Art. 6 Abs. 1 bzw. Art. 9 Abs. 2 DSGVO.⁹¹

II. Weitergabe nicht-personenbezogener Daten

Sofern die im Rahmen des Projekts ausgetauschten und weitergegebenen Daten keine personenbezogenen im Sinne der DSGVO darstellen, müssen die Projektpartner bei deren Weitergabe *lediglich* die Vertraulichkeitsvereinbarungen und möglicherweise bestehenden Geschäftsgeheimnisse beachten.⁹²

E. Schutz von Geschäftsgeheimnissen

Innerhalb des Projekts K3I-Cycling ist der Schutz von Geschäftsgeheimnissen für die Beteiligten von großer Bedeutung. In dem Kooperationsvertrag finden sich mehrere Passagen (Ziffer 5, Ziffer 7.2, Ziffer 8.3) die ausdrücklich auf die Vertraulichkeit der im Projekt für geheimhaltungsbedürftig erklärten Informationen Bezug nehmen. Fraglich ist, ob diese Vertraulichkeitsklauseln ausreichen, um einen umfassenden Schutz von Geschäftsgeheimnissen gewährleisten zu können und wie sich das neue Geschäftsgeheimnisgesetz (GeschGehG) auswirkt.

I. Abstrakte Ausführungen

Vorab ist festzuhalten, dass es an einer die **Verkehrsfähigkeit** von Geschäftsgeheimnissen regelnden Vorschrift **fehlt**.⁹³ Es fehlt an einer Norm mit einer konkreten Aussage zur Existenz eines subjektiven absoluten Rechts an Geschäftsgeheimnissen und deren Übertragbarkeit.⁹⁴ Folglich ist davon auszugehen, dass es sich bei diesen zwar um immaterielle Güter, oft mit Vermögenswert, handelt, jedoch

⁸⁸ Bronner/Wiedemann, Rechtmäßigkeit der Datenverarbeitung bei wissenschaftlicher Forschung an staatlichen Hochschulen, ZD 2023, 77, 81.

⁸⁹ Specht-Riemenschneider/Wehde, Forschungsdatenzugang, ZGI 2022, 3, 7.

⁹⁰ Bronner/Wiedemann, Rechtmäßigkeit der Datenverarbeitung bei wissenschaftlicher Forschung an staatlichen Hochschulen, ZD 2023, 77, 81; Herbst, in: Kühling/Buchner, Art. 5 Rn. 49a; DSK, Erfahrungsbericht zur Anwendung der DS-GVO, November 2019, S. 13.

⁹¹ Bronner/Wiedemann, Rechtmäßigkeit der Datenverarbeitung bei wissenschaftlicher Forschung an staatlichen Hochschulen, ZD 2023, 77, 81.

⁹² Der Schutz von Geschäftsgeheimnissen wird im nächsten Abschnitt näher beleuchtet werden.

⁹³ Slawik, in: Brammsen/Apel GeschGehG, 2022, Einl. D Rn. 2.

⁹⁴ Slawik, in: Brammsen/Apel, Einl. D Rn. 2.

nicht um Objekte eines Immaterialgüterrechts mit Ausschließlichkeitwirkung.⁹⁵ Sofern, wie vorliegend, eine solche ausschließliche Wirkweise angestrebt wird, muss diese durch entsprechende vertragliche Vereinbarungen, insbesondere durch Vertraulichkeitsverpflichtungen und Nutzungsbeschränkungen⁹⁶, *abgesichert* werden.

1. Begriffsbestimmung „Geschäftsgeheimnis“

Der Begriff des Geschäftsgeheimnisses wird seit Inkrafttreten des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG)⁹⁷ am 26.4.2019 erstmalig definiert. Nach **§ 2 S. 1 Nr. 1 GeschGehG** ist ein Geschäftsgeheimnis eine Information, die nicht allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und die Gegenstand von den Umständen angemessenen Geheimhaltungsmaßnahmen ist. Als schützenswert erachtet werden beispielsweise Forschungsprojekte⁹⁸, Entwicklungsunterlagen⁹⁹, Datenmodelle/-sätze¹⁰⁰ sowie Algorithmen¹⁰¹ und Prototypen¹⁰².

a) Information

Unter dem Begriff „Information“ im Sinne dieser Begriffsbestimmung wird das **Wissen um eine Tatsache** verstanden.¹⁰³ Dabei kann es sich um Geschehnisse, Verhältnisse oder Zustände der Vergangenheit oder Gegenwart handeln.¹⁰⁴ Im Gegensatz beispielsweise zum Urheberrecht sind die Individualität, Neuheit oder Schöpfungshöhe keine Voraussetzung.¹⁰⁵ Es bedarf zusätzlich **keiner menschlichen Schöpfungsleistung**, weswegen auch maschinengenerierte Daten grundsätzlich als Geschäftsgeheimnisse eingestuft werden können, sofern die weiteren Voraussetzungen des § 2 Nr. 1 GeschGehG vorliegen.¹⁰⁶ Der Schutz wird auch unabhängig davon gewährleistet, ob das Geheimnis in irgendeiner Form verkörpert oder nur im virtuellen Raum vorhanden ist.¹⁰⁷

⁹⁵ *Slawik*, in: Brammsen/Apel, Einl. D Rn. 2, § 1 Rn. 12.

⁹⁶ *Slawik*, in: Brammsen/Apel, Einl. D Rn. 2.

⁹⁷ Dessen Entwicklung resultiert aus der europäischen Geheimnisschutzrichtlinie vom 08.06.2016, RL (EU) 2016/934, welche den nationalen Gesetzgebern aufgab, die Vorgaben der Richtlinie in nationales Recht umzusetzen.

⁹⁸ OLG Brandenburg, Beschl. v. 10.7.2017 – 6 Kart 1/17, RdE 2017, 547 Rn. 53; OVG Münster, Urt. v. 18.8.2015 – 15 A 97/13, NVwZ 2016, 1025 Rn. 75 ff.

⁹⁹ BVerfG, Urt. v. 21.10.2014 – 2 BvE 5/11, NVwZ 2014, 1652 Rn. 182.

¹⁰⁰ OLG Jena, Urt. v. 8.12.2015 – 5 U 1042/12, NJOZ 2016, 175, Rn. 69, 77, 87.

¹⁰¹ BGH, Urt. v. 28.1.2014 – VI UR 156/13, DGVZ 2014, 145 (147); OLG München, Urt. v. 27.02.2020 – 29 U 2584/19, WRP 2020, 654 Rn. 26.

¹⁰² BGH, Urt. v. 18.2.1977 – I ZR 112/75, GRUR 1977, 539 (539ff.).

¹⁰³ *Hiéramente*, in: BeckOK GeschGehG, 26. Ed., Stand: 01.03.2025, GeschGehG § 2 Rn. 2

¹⁰⁴ *Hiéramente*, in: BeckOK GeschGehG, GeschGehG § 2 Rn. 2.

¹⁰⁵ *Alexander*, Geschäftsgeheimnisse und Ranking-Transparenz, MMR 2021, 690, 691, wobei die Information bei Fehlen solcher Eigenschaften aus einem anderen Grund nicht schützenswert sein kann, zB mangels geheimer Natur: *Hiéramente*, in: BeckOK GeschGehG, GeschGehG § 2 Rn. 2.

¹⁰⁶ *Hessel/Leffer*, Rechtlicher Schutz maschinengenerierter Daten, MMR 2020, 647, 648 f.

¹⁰⁷ *Alexander*, in: Köhler/Feddersen UWG, 44. Aufl. 2026, GeschGehG § 2 Rn. 25a; in best. Normen des GeschGehG wird allerdings eine Verkörperung vorausgesetzt.

b) *Fehlende Bekanntheit der Information*

Nicht unter den Begriff des Geschäftsgeheimnisses fallen Informationen, die den Personenkreisen, die üblicherweise mit solchen Informationen umgehen, **allgemein bekannt** oder **leicht zugänglich** sind.¹⁰⁸ **Allgemein bekannt** sind Tatsachen, die ohne Weiteres zugänglich sind.¹⁰⁹ **Ohne Weiteres zugänglich** sind Informationen, von denen sich Interessierte ohne größeren Zeit- und Kostenaufwand¹¹⁰ und mit lauterem Mitteln¹¹¹ Kenntnis verschaffen können.¹¹² Auch Datensammlungen, in denen unter anderem auch öffentlich zugängliche Angaben zusammentragen sind, können schützenswert sein, da sich ihre Geheimnisqualität aus der Strukturierung ergeben kann.¹¹³ An der fehlenden Bekanntheit ändert auch die Offenlegung der Information gegenüber einem **ausgewählten Personenkreis** nichts.¹¹⁴ *Dementsprechend ändert auch die Tatsache, dass bei K3I-Cycling mehrere Projektpartner untereinander Informationen austauschen, nichts an deren Geheimheit.*

c) *Wirtschaftlicher Wert der Information*

Die zu schützende Information muss auch von wirtschaftlichem Interesse sein bzw. einen wirtschaftlichen Wert haben. Dieses Interesse wird zwar vom europäischen Gesetzgeber nicht definiert, allerdings durch Beispiele in Erwägungsgrund 14 zur Richtlinie¹¹⁵ konkretisiert. Demnach muss die Information einen **realen oder potenziellen Handelswert** haben. Dies soll aber wiederum nicht so verstanden werden, dass ein Geheimnis nur dann wirtschaftlichen Wert hat, wenn es auf dem Markt kommerzialisierbar ist.¹¹⁶ Einer Information wird dann ein wirtschaftlicher Wert zugeschrieben, „wenn ihre Erlangung, Nutzung oder Offenlegung ohne Zustimmung des Inhabers dessen wissenschaftliches oder technisches Potenzial, geschäftliche oder finanzielle Interessen, strategische Positionen oder Wettbewerbsfähigkeit negativ beeinflussen kann“.¹¹⁷ Darunter können auch Informationen fallen, die für Dritte keinen klassischen wirtschaftlichen Wert haben und dementsprechend nicht im engeren Sinne „kommerzialisierbar“ sind.¹¹⁸ Es ist **nicht erforderlich**, dass die Information einen bestimmten, **beziehbaren Vermögenswert** hat¹¹⁹, sondern ausreichend, wenn es sich für den

¹⁰⁸ Regierungsentwurf zur Umsetzung der Richtlinie EU 2016/943, BT-Drs. 19/4724, S. 24; OLG Schleswig, Urt. v. 28.04.2022 – 6 U 39/21, GRUR-RS 2022, 9007, Rn. 42.

¹⁰⁹ *Harte-Bavendamm*, in: Harte-Bavendamm/Ohly/Kalbfus GeschGehG, 2. Aufl. 2024, § 2 Rn. 30.

¹¹⁰ Es existieren keine genauen Angaben zum Umfang; jedenfalls dann nicht geheim, wenn sich die Information innerhalb weniger Stunden beschaffen lässt, *Hiéramente* in BeckOK GeschGehG, § 2 Rn. 9.

¹¹¹ *Harte-Bavendamm*, in: Harte-Bavendamm/Ohly/Kalbfus, § 2 Rn. 30.

¹¹² OLG Düsseldorf, Urt. v. 11.3.2021 – I-15 U 6/20, WRP 2021, 1080, Rn. 28.

¹¹³ OLG Hamm, Urt. v. 23.06.2021 – 10 SaGa 9/21, BeckRS 2021, 41734 Rn. 14; *Hiéramente*, in: BeckOK GeschGehG, § 2 Rn. 8.

¹¹⁴ *Hiéramente*, in: BeckOK GeschGehG, § 2 Rn. 10.

¹¹⁵ Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, abrufbar unter: [RICHTLINIE \(EU\) 2016/ 943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES - vom 8. Juni 2016 - über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen \(Geschäftsgeheimnisse\) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung](#)

¹¹⁶ *Glinke*, in: Keller/Schönknecht/Glinke, Geschäftsgeheimnisschutzgesetz, 1. Aufl. 2021, § 2 Rn. 46.

¹¹⁷ *Glinke*, in: Keller/Schönknecht/Glinke, § 2 Rn. 46; BT-Drucksache 19/4724, S. 22.

¹¹⁸ *Glinke*, in: Keller/Schönknecht/Glinke, § 2 Rn. 46.

¹¹⁹ *Glinke*, in: Keller/Schönknecht/Glinke, § 2 Rn. 47.

Geheimnisschutzsuchenden nachteilig auswirken kann, wenn Dritte Kenntnis von den Informationen erlangen.¹²⁰ Es muss auch eine **Verknüpfung** zwischen wirtschaftlichem Wert und Geheimhaltungsinteresse dahingehend bestehen, dass der wirtschaftliche Wert zumindest auch darauf zurückzuführen sein muss, dass die Information nicht allgemein bekannt ist.¹²¹ Denn der Geheimnisinhaber muss zumindest ein **legitimes Interesse** an der Geheimhaltung haben.¹²²

d) Angemessene Geheimhaltungsmaßnahmen

Damit ein Geschäftsgeheimnis im Sinne des GeschGehG gegeben ist, muss die zu schützende Information weiterhin Gegenstand angemessener Geheimhaltungsmaßnahmen sein. Diese Notwendigkeit der Gewährleistung eines angemessenen Schutzniveaus durch den Geheimnisinhaber stellt insgesamt eine Verschärfung der Anforderungen gegenüber der alten Rechtslage vor Einführung des GeschGehG dar. Hat zuvor ein — grundsätzlich vermuteter – Geheimhaltungswille genügt, um die zu schützende Information als Geschäftsgeheimnis einzuordnen, muss dieser Wille nunmehr durch die Ergreifung entsprechender Maßnahmen hinreichend dokumentiert werden.¹²³ Welche Geheimhaltungsmaßnahmen als angemessen iSd GeschGehG anzusehen sind, ist dabei stets von den jeweils konkreten Umständen des Einzelfalls abhängig.¹²⁴ Grundlegend lassen sich in der Praxis dabei insbesondere drei Arten möglicher Geheimhaltungsmaßnahmen unterscheiden, rechtliche, organisatorische sowie technische Maßnahmen.¹²⁵ Welche konkreten Maßnahmen für den Schutz von Geschäftsgeheimnissen in digitalen Zwillingen wie dem ANT in Betracht kommen, um ein angemessenes Schutzniveau sicher zu stellen, wurde in einem im Rahmen des Projekts veröffentlichten Fachbeitrag näher erläutert, auf welchen an dieser Stelle verwiesen wird.

e) Berechtigtes Interesse an der Geheimhaltung

Das im Rahmen des § 2 Nr. 1 GeschGehG weiterhin geforderte berechtigte Interesse an der Geheimhaltung der Information wird weitgehend als lediglich zusätzliches Merkmal angesehen, welches dazu dient, reine Bagatellfälle aus dem Schutzbereich des GeschGehG herauszunehmen.¹²⁶ Dem Merkmal des berechtigten Interesses an der Geheimhaltung kommt daher in der Praxis nur eine untergeordnete Rolle zu.

¹²⁰ BGH, Urt. v. 27.4.2006 – I ZR 126/03, GRUR 2006, 1044 Rn. 19; *Glinke*, in: Keller/Schönknecht/Glinke, § 2 Rn. 47.

¹²¹ *Harte-Bavendamm*, in: Harte-Bavendamm/Ohly/Kalbfus, § 2 Rn. 37; *Glinke*, in: Keller/Schönknecht/Glinke, § 2 Rn. 49.

¹²² *Glinke* in: Keller/Schönknecht/Glinke, § 2 Rn. 49.

¹²³ *Arens*, Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) - neue Herausforderungen für den Geschäftsführer, GWR 2019, 375, 376.

¹²⁴ *Alexander*, in: Köhler/Feddersen, UWG, § 2 GeschGehG Rn. 66.

¹²⁵ *Hessel/Leffer*, Rechtlicher Schutz maschinengenerierter Daten, MMR 2020, 647, 649.

¹²⁶ *Hiéramente*, in: BeckOK GeschGehG, § 2 GeschGehG Rn. 71.

2. Unterscheidung Vertraulichkeitsvereinbarung und Vertraulichkeitsklauseln

Eine **Vertraulichkeitsvereinbarung** wird regelmäßig im Vorfeld des Abschlusses eines Hauptvertrags getroffen, um die Parteien auch vor dessen Finalisierung schon hinsichtlich der geteilten und zur Verfügung gestellten Informationen zu schützen.¹²⁷ Im Gegensatz dazu handelt es sich bei **Vertraulichkeitsklauseln** nicht um eigenständige Verträge, sondern um Klauseln, die einen Bestandteil des Hauptvertrags bilden.¹²⁸ Die Parteien sind zwar auch ohne solche Klauseln in der Regel zu einer gewissen Vertraulichkeit verpflichtet, was aus der vertraglichen Pflicht zur Rücksichtnahme aus § 241 Abs. 2 BGB resultiert¹²⁹, eine explizite Regelung führt aber zur Gewissheit über Inhalt und Grenzen dieser Verpflichtung und schafft im Falle einer Verletzung dieser Pflicht auch eine eindeutige Haftungsgrundlage.¹³⁰ Der Abschluss einer ausdrücklichen Regelung ist daher immer vorzugswürdig. Die Definition der geschützten oder geheimhaltungsbedürftigen vertraglichen Informationen gehen regelmäßig über den gesetzlichen Begriff des Geschäftsgeheimnisses hinaus.¹³¹

3. Auswirkungen des GeschGehG

Es stellt sich die Frage, ob angesichts der Möglichkeit des Abschlusses solcher Vertraulichkeitsvereinbarungen/-klauseln das GeschGehG überhaupt noch darüber hinausgehende Auswirkungen mit sich bringt. Es werden allerdings mehrere Bereiche diskutiert, in denen das Geschäftsgeheimnis durchaus Konsequenzen auf die Ausgestaltung von Vereinbarungen zum Schutz der Vertraulichkeit hat.

Zum einen sieht das GeschGehG vor, dass, damit ein im Sinne dieses Gesetzes geschütztes Geschäftsgeheimnis vorliegt, dieses nach § 2 Nr. 1 lit. b durch angemessene Geheimhaltungsmaßnahmen zu schützen ist.¹³² Hierzu können auch vertragliche Abreden, wie Vertraulichkeitsklauseln, zählen.¹³³ In der Praxis sind solche Vertraulichkeitsvereinbarungen jedoch regelmäßig so weit gefasst und nicht hinreichend konkretisiert, welche Geschäftsgeheimnisse konkret zu wahren sind, dass solche Vereinbarungen regelmäßig keine angemessenen Maßnahmen zur Geheimhaltung darstellen.¹³⁴ Wenn die Parteien den Schutz des GeschGehG erlangen möchten, besteht dann ein dahingehender Konkretisierungsbedarf, der in Form des Abschlusses einer entsprechenden zusätzlichen Vereinbarung umgesetzt werden könnte.

¹²⁷ Slawik, in: Brammsen/Apel, Einl. D Rn. 5; zu den einzelnen Erscheinungsformen von Vertraulichkeitsvereinbarungen.

¹²⁸ Slawik, in: Brammsen/Apel, Einl. D Rn. 25.

¹²⁹ BAG, Urt. v. 17.10.2024 – 8 AZR 172/23, NZA 2025, 112 Rn. 42 hinsichtlich einer arbeitsrechtlichen Haftung; von Busekist/Racky, Hinweisgeber- und Geschäftsgeheimnisschutz – ein gelungener Referentenentwurf, ZRP 2018, 135, 137; Slawik, in: Brammsen/Apel, Einl. D Rn. 27.

¹³⁰ Slawik, in: Brammsen/Apel, Einl. D Rn. 27.

¹³¹ Kalbfus/Harte-Bavendamm, in: Harte-Bavendamm/Ohly/Kalbfus, Einl. Teil B, Rn. 29.

¹³² Brammsen, in: Brammsen/Apel, § 2 Rn. 57.

¹³³ Jansen/Hofmann, Auswirkungen des Gesetzes zum Schutz von Geschäftsgeheimnissen auf Vertraulichkeitsvereinbarungen, BB 2020, 259, 260f..

¹³⁴ Freckmann/Scholl, Geheimnisschutzrichtlinie: Neuer Standard für Vertraulichkeitsvereinbarungen und arbeitsvertragliche Verschwiegenheitsklauseln, BB 2017, 1780 (1782).

Es ist daher bereits an dieser Stelle festzuhalten, dass den Beteiligten bei K3I-Cycling der Abschluss entsprechender Vereinbarungen zu empfehlen ist. Eine Vertraulichkeitsklausel wurde mit Ziffer 5 des Kooperationsvertrags zum Verbundvorhaben K3I-Cycling getroffen. Diese dürfte aber für einen Geschäftsgeheimnisschutz für sich genommen noch nicht ausreichend sein, sondern sollte um eine explizite Geschäftsgeheimnisvereinbarung ergänzt werden.

F. Nutzungsrechte an den entstehenden Produkten

Um beurteilen zu können, wem welche Nutzungsrechte an den entstehenden Produkten, insbesondere des Artificial Neural Twins (ANTs) zustehen können, ist zunächst die Frage nach deren Schutzfähigkeit zu beantworten.

I. Der Artificial Neural Twin

II. Schutzfähigkeit des ANTs

Hinsichtlich der Schutzfähigkeit des ANTs ist zwischen dem *Datenkonstrukt/KI-System(Softwarecode)* an sich und der Schutzfähigkeit des generierten Outputs zu unterscheiden.

1. Schutz des ANTs als KI-System

a) Urheberrechtlicher Schutz

Der ANT könnte als *Computerprogramm* nach dem UrhG schutzfähig sein. Dazu müsste es sich dabei um ein Computerprogramm nach §§ 2 Abs. 1 Nr. 1, 69a UrhG handeln. Dieser Begriff wird vom UrhG zwar nicht legaldefiniert, mittlerweile hat sich jedoch in der *Literatur und Rechtsprechung* ein Begriffsverständnis entwickelt, wonach darunter „eine Reihe von Befehlsanweisungen an einen Computer zur Erzielung einer Wirkung zu verstehen“ verstanden wird.¹³⁵

Beim *Einsatz von Technologien der Künstlichen Intelligenz* ist bei *Expertensystemen*¹³⁶, zwischen der Dialogkomponente, der Interferenzmaschine und der Wissenskomponente zu unterscheiden. Mithilfe der Dialogkomponente als Bestandteil des Systems kann der Nutzer diese befragen oder der Experte Wissen einspeisen.¹³⁷ Die Interferenzmaschine soll den Teil des Systems erfassen, der die Regeln enthält, nach denen aus dem antrainierten und gespeicherten Wissen Schlüsse gezogen werden können.¹³⁸ Die Wissenskomponente enthält das eigentliche Wissen des Systems, dargestellt in

¹³⁵ KG Berlin, Urt. v. 17.03.2010 – 24 U 117/08 - juris, Rn. 46.

¹³⁶ So *Grützmaker*, in: Wandtke/Bullinger, Urheberrecht, 6. Aufl. 2022, UrhG § 69a Rn. 21; LG Oldenburg (Oldenburg), Urteil vom 31. Januar 1996 – 5 O 3578/93, CR 1996, 217, 219 f.; *Dreier*, in: Dreier/Schulze UrhG, 8. Auflage 2025, § 69a Rn. 12.

¹³⁷ *Grützmaker*, in: Wandtke/Bullinger, UrhG § 69a Rn. 21.

¹³⁸ Ebenda.

strukturierter Form und komplexen Datensätzen.¹³⁹ Diese kann allenfalls als Datenbank geschützt sein.¹⁴⁰

Unabhängig von der jeweiligen Komponente fordert das UrhG jedoch nach §§ 2 II, 69a III 1 UrhG eine persönliche geistige Schöpfung und damit eine hinreichende Schöpfungshöhe, also eine vom menschlichen Urheber vorgenommene hinreichend individuelle Prägung.¹⁴¹ Übertragen auf Softwarecode ist eine solche Schöpfungshöhe, an die grundsätzlich nicht allzu hohe Anforderungen gestellt werden („kleine Münze“ des Urheberrechts¹⁴²), erfüllt bei einer eigenpersönlichen Nutzung eines bestehenden Gestaltungsspielraums insbesondere bezogen auf „Art und Form der Sammlung, [Anordnung und Einteilung] des Materials bei der Problemanalyse [sowie] der Erstellung des Datenfluss- und Programmablaufplans“.¹⁴³ Der urheberrechtliche Schutz ist erst bei banaler und routinemäßiger Programmierleistung nicht mehr gegeben, soweit diese auch von jedem Programmierer in vergleichbarer Art und Weise umgesetzt werden könnte.¹⁴⁴ Geschützt werden sowohl der Quell¹⁴⁵- als auch der Objektcode¹⁴⁶. Es bedarf jedoch einer menschlichen Gestaltungsentscheidung; die technischen Werkzeuge dürfen lediglich als Hilfsmittel bei der Umsetzung des Gestaltungsakts eingesetzt werden.¹⁴⁷ Eine vollständige Vorhersehbarkeit des Endergebnisses ist jedoch nicht erforderlich, da diese auch bei „klassischen“ Schöpfungsprozessen nicht immer gegeben sein muss.¹⁴⁸

Daher stellt sich die Frage, ab welchem Einfluss des (technischen) Hilfsmittels nicht mehr von einem menschlichen Schöpfungsvorgang gesprochen werden kann.

Einige Stimmen aus der Literatur wollen diese Frage mithilfe des Erfordernisses einer entsprechenden menschlichen Zurechnung beantworten. Der Schaffensprozess soll vom Menschen nicht vollständig aus der Hand gegeben werden dürfen.¹⁴⁹ Sofern eine Handlung, in Form des Ingangsetzens des entsprechenden Programms, zwar letztlich zu einem Ergebnis, einer Werkentstehung, führt, ist sie von völlig untergeordneter Bedeutung, weil der Algorithmus dann alle wesentlichen Kreativitätsentscheidungen trifft. Die menschliche Handlung ist dann nicht von entscheidender

¹³⁹ Ebenda.

¹⁴⁰ *Grützmacher*, in: Wandtke/Bullinger, UrhG § 69a Rn. 21.

¹⁴¹ *Apel/Kaulartz*, Rechtlicher Schutz von Machine-Learning-Modellen, RD 2020, 24, 27 Rn. 14.

¹⁴² BGH Urt. v. 13.11.2013 – I ZR 143/12, GRUR 2014, 175, 176 Rn. 18.

¹⁴³ KG Berlin Urt. v. 6.9.2010 – 24 U 71/10, ZUM-RD 2011, 544, 547; *Dreier*, in: Dreier/Schulze, § 69a Rn. 26.

¹⁴⁴ OLG München Urt. v. 27.5.1999 – 6 U 5497/98, ZUM-RD 1999, 445, 447; KG Berlin Urt. v. 6.9.2010 – 24 U 71/10, ZUM-RD 2011, 544, 547; *Specht-Riemenschneider*, Urheberrechtlicher Schutz für Algorithmen-erzeugnisse? – Phasenmodell de lege lata, Investitionsschutz de lege ferenda?, WRP 2021, 273, 274.

¹⁴⁵ Quellcode entsteht, wenn der Programmablauf durch Anwendung der Programmiersprache in eine Befehlsfolge umgewandelt wird, die für den Computer lesbar ist; BGH Urt. v. 9.5.1985 – I ZR 52/83, GRUR 1985, 1041, 1046 f..

¹⁴⁶ Objektcode ist ein Zwischenergebnis eines Compiler- bzw. Übersetzungsvorgangs von einem Programm, *Schmidt* in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, Teil A § 1 Rn. 162.

¹⁴⁷ *Specht-Riemenschneider*, Urheberrechtlicher Schutz für Algorithmen-erzeugnisse? – Phasenmodell de lege lata, Investitionsschutz de lege ferenda?, WRP 2021, 273, 274.

¹⁴⁸ So zB beim Action Painting, *Specht-Riemenschneider*, Urheberrechtlicher Schutz für Algorithmen-erzeugnisse? – Phasenmodell de lege lata, Investitionsschutz de lege ferenda?, WRP 2021, 273, 275.

¹⁴⁹ *Hetmank/Lauber-Rönsberg*, Künstliche Intelligenz – Herausforderungen für das Immaterialgüterrecht, GRUR 2018, 574, 577; *Loewenheim/Leistner*, in: Schricker/Loewenheim UrhG, 6. Aufl. 2020, § 2 Rn. 39 ff.

Bedeutung, weil sich das System selbständig fortentwickelt und dementsprechend ihr Erzeugnis einer menschlichen Einflussnahme nicht mehr zugeschrieben werden kann.

Demnach sind beispielsweise solche Algorithmen, die auf einer höheren Allgemeinheitsstufe stehen und sich als Lösung für bestimmte Aufgaben und Probleme etabliert haben, nicht schutzfähig, zumal sie zum Standardrepertoire der Programmier Technik gehören; womit es an der Individualität mangelt.¹⁵⁰ Damit ist allerdings nicht ausgeschlossen, dass die konkrete Anordnung der in dem Modell enthaltenen Algorithmen oder die konkrete Zusammensetzung eines Modells bei hinreichender Schöpfungshöhe urheberrechtlich schutzfähig sein kann.¹⁵¹

b) Schutz als Datenbank

Der ANT könnte jedoch unter Umständen als **Datenbankwerk** iSv § 4 Abs. 1 und 2 UrhG schutzfähig sein. Der Begriff der „Datenbank“ ist in § 87a Abs. 1 S. 1 UrhG legaldefiniert und danach eine „Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder in anderer Weise zugänglich sind“.

2. Patentrechtlicher Schutz

Der ANT könnte patentfähig und damit nach entsprechender Anmeldung schutzfähig sein. Patente werden nach § 1 Abs. 1 PatG für Erfindungen auf jedem Gebiet der Technik erteilt, wenn sie auf einer erfinderischen Tätigkeit beruhen, neu sind und gewerblich anwendbar sind. Nach § 3 Abs. 1 PatG gilt eine Erfindung dann als neu, wenn sie nicht zum Stand der Technik gehört, wobei dieser alle Kenntnisse umfasst, die vor dem für die Anmeldung maßgeblichen Tag durch schriftliche oder mündliche Beschreibung, Benutzung oder in sonstiger Weise der Öffentlichkeit zugänglich gemacht wurden. Jedoch könnte der ANT als Computerprogramm und damit „Programm für Datenverarbeitungsanlagen“ iSv § 1 Abs. 3 Nr. 3 PatG *gerade nicht* als Erfindung anzusehen sein.

Zu beachten ist außerdem, dass ab dem Tag der Veröffentlichung eine Patentierbarkeit nicht mehr möglich ist.

a) Problem der Technizität

Denn Patentschutz soll nur dann gewährt werden, wenn über die Verarbeitung des betreffenden Programms durch einen Computer hinaus eine **Technizität** dergestalt hinzutritt, dass das Computerprogramm neben der Datenverarbeitung einen weiteren technischen Effekt erzeugt oder ein

¹⁵⁰ Spindler, in: Schricker/Loewenheim, § 69a Rn. 12aff.

¹⁵¹ Ehinger/Stiemerling Die urheberrechtliche Schutzfähigkeit von Künstlicher Intelligenz am Beispiel von Neuronalen Netzen, CR 2018, 761, Rn. 43 f., 66; Bischof/Intveen, Einsatz künstlicher Intelligenz durch Unternehmen, ITRB 2019, 134, 136; Hartmann/Prinz, Immaterialgüterrechtlicher Schutz von Systemen Künstlicher Intelligenz, WRP 2018, 1431, Rn. 29 ff.

technisches Problem löst, sog. computerimplementierte Erfindung.¹⁵² Einem Computerprogramm als solches, welches das KI-System operabel macht, soll aufgrund des fehlenden technischen Charakters grundsätzlich kein patentrechtlicher Schutz zugutekommen.¹⁵³

Überdies bedürfte es, auch bei unterstellter vorhandener Technizität, einer erfinderischen Tätigkeit **durch einen Menschen**, die beim Einsatz von KI-Systemen teilweise anzuzweifeln ist.¹⁵⁴ Zu unterscheiden ist zwischen KI-Erfindungen und menschlichen Erfindungen. „KI-Erfindungen“ sind solche technischen Entwicklungen, die KI-induziert sind.¹⁵⁵ Hinsichtlich solcher KI-Erfindungen stellt sich die Frage nach der Patentierbarkeit aufgrund der Tatsache, dass die KI mit dem „Erfinder“-Begriff aus § 6 PatG nur schwer in Einklang zu bringen ist.¹⁵⁶ Soweit die KI nur als Werkzeug verwendet wird und noch eine menschliche schöpferische Tätigkeit besteht, kann als Erfinder im Sinne des PatentG anerkannt werden, „wer durch Programmgestaltung und Auswertung der Ergebnisse des Computers die Lösung der technischen Problemstellung erreicht und erkennt“.¹⁵⁷ Werden hingegen technische Lösungen durch eine KI geschaffen, deren Ergebnisse sich aufgrund ihrer Eigenschaften nicht mehr vorhersehen lassen und die auch für Fachleute nicht nachvollziehbar sind, mangelt es an einer menschlichen Erfindung.¹⁵⁸ Diskutiert wird in der Literatur aus diesem Grund, ob der Begriff des Erfinders bzw. der Erfindung im Patentrecht eine Reform benötigt bzw. von dem Schöpfungsbegriff aus dem Urheberrecht bewusst abzukoppeln.¹⁵⁹ Hinsichtlich des ANTs gilt, dass dieser zwar, sobald er zur Optimierung eingesetzt wird, vollständig automatisch arbeitet. Würde mithin in dieser Phase eine technische Entwicklung, die die Voraussetzungen einer Erfindung erfüllt, entstehen, wäre diese wohl eine KI-Erfindung, da die Entscheidungsprozesse des ANT nicht mehr nachvollziehbar sind. Dieses Szenario ist jedoch sehr unwahrscheinlich.

Die hier betrachtete Patentierbarkeit des ANT bezieht sich auf dessen Entwicklung. Der ANT wird durch einen Menschen entworfen bzw. geschaffen. Fraglich ist letztlich nur, ob die sonstigen Voraussetzungen einer Erfindung vorliegen.

¹⁵² BGH, Urt. v. 24.2.2011 – X ZR 121/09, MMR 2011, 540 Rn. 15; *Sattler* in *Rechtshandbuch Industrie 4.0 und Internet of Things*, Kap. 2, § 2, Rn. 23; *Ménière/Pihlajamaa*, Künstliche Intelligenz in der Praxis des EPA, GRUR 2019, 332, 334.

¹⁵³ *Tochtermann*, in: Kaulartz/Braegelmann, *Rechts-HdB Artificial Intelligence und Machine Learning*, Kap. 7.3, Rn. 8.

¹⁵⁴ *Konertz/Schönhof* Erfindungen durch Computer und künstliche Intelligenz – eine aktuelle Herausforderung für das Patentrecht?, ZGE 2018, 380, 411; *Stierle*, Artificial Intelligence Designated as Inventor – An Analysis of the Recent EPO Case Law, GRUR-Int 2020, 918, 923.

¹⁵⁵ Siehe hierzu: *Wiebe*, in: Leupold/Wiebe/Glossner, *IT-Recht*, 4. Auflage 2021, Teil 9.6.1 Rn. 9 ff.

¹⁵⁶ *Wiebe*, in: Leupold/Wiebe/Glossner, Teil 9.6.1 Rn. 10.

¹⁵⁷ A.a.O.; *Melullis*, in: Benkard, *PatG*, 12. Auflage 2023, § 6 Rn. 32.

¹⁵⁸ *Wiebe*, in: Leupold/Wiebe/Glossner, Teil 9.6.1 Rn. 10.

¹⁵⁹ *Wiebe* spricht von einer möglichen Objektivierung des Erfindungsbegriffs, *Wiebe*, in: Leupold/Wiebe/Glossner, Teil 9.6.1 Rn. 13; siehe auch: *Konertz/Schönhof*, Erfindungen durch Computer und künstliche Intelligenz – eine aktuelle Herausforderung für das Patentrecht?, ZGE 2018, 380, 411.

3. Know-How-Schutz

Dem ANT könnte, anknüpfend an obige Ausführungen zur Bedeutung des GeschGehG im Rahmen des Projekts, jedoch ein sog. „Know How“ oder Geschäftsgeheimnis-Schutz zukommen.

a) Schutzvoraussetzungen im konkreten Fall

Um in den Schutzbereich des GeschGehG zu kommen, müsste der ANT als Geschäftsgeheimnis qualifiziert werden. Dabei genügt, wie oben bereits erwähnt, nicht mehr nur der subjektive Geheimhaltungswille und ein Geheimhaltungsinteresse, sondern es bedarf neben einem erforderlichen berechtigten Interesse, § 2 Abs. 1 lit. c GeschGehG, auch angemessener Geheimhaltungsmaßnahmen, § 2 Abs. 1 lit. c GeschGehG. Diese sollen letztlich den Geheimhaltungswillen objektiv dokumentieren.¹⁶⁰ Überdies muss das Geschäftsgeheimnis speziell wegen seiner Geheimheit ein wirtschaftlicher Wert zugesprochen werden, § 2 Abs. 1 lit. a GeschGehG.¹⁶¹ Dies dürfte im Zusammenhang mit künstlicher Intelligenz regelmäßig der Fall sein.¹⁶²

b) Angemessene Schutzmaßnahmen

Wie genau angemessene Schutzmaßnahmen iSd GeschGehG aussehen müssen, überlässt der Gesetzgeber demjenigen, der den Schutz in Anspruch nehmen möchte. Es findet sich allerdings der Hinweis, dass die Maßnahmen „angemessen“ sein müssen. Maßgeblich sind laut der Gesetzgebung der Wert des Geschäftsgeheimnisses, dessen Entwicklungskosten sowie die Natur der Informationen, die Bedeutung für das Unternehmen, dessen Größe und übliche Geheimhaltungsmaßnahmen sowie vereinbarte vertragliche Regelungen mit Arbeitnehmern und Geschäftspartnern als auch das Gefährdungspotenzial.¹⁶³ In der Praxis ließe sich dies etwa umsetzen durch das Vorsehen von Zugriffsrechten sowie Verschlüsselungen und einer Verpflichtung der Geschäftspartner zu Verschwiegenheit.¹⁶⁴

III. Gefahr von Social-Engineering-Angriffen

Bei einem Social-Engineering-Angriff möchte der Angreifer sein Opfer dazu bringen, ihm versehentlich oder auch absichtlich in gutem Glauben sensitive Informationen zur Verfügung zu stellen.¹⁶⁵ Es handelt sich hierbei um nichttechnische Angriffe.¹⁶⁶ Entsprechende Angriffe sind auch im Projektszenario denkbar. So besteht beispielsweise die Möglichkeit für Mitarbeiter von Entsorgungsunternehmen

¹⁶⁰ Ohly, Das neue Geschäftsgeheimnisgesetz im Überblick, GRUR 2019, 441, 443; Kalbfus Angemessene Geheimhaltungsmaßnahmen nach der Geschäftsgeheimnis-Richtlinie, GRUR-Prax 2017, 391, 391.

¹⁶¹ Harte-Bavendamm, in: Harte-Bavendamm/Ohly/Kalbfus § 2 Rn. 37.

¹⁶² Apel/Kaulartz, Rechtlicher Schutz von Machine Learning-Modellen, RDi 2020, 24, 30, m.w.N..

¹⁶³ BT-Drs. 19/4724, S. 25; Apel/Kaulartz, Rechtlicher Schutz von Machine Learning-Modellen, RDi 2020, 24, 30; Maaßen, „Angemessene Geheimhaltungsmaßnahmen“ für Geschäftsgeheimnisse, GRUR 2019, 352, 355.

¹⁶⁴ Apel/Kaulartz, Rechtlicher Schutz von Machine Learning-Modellen, RDi 2020, 24, 31 f.

¹⁶⁵ Eckert, IT-Sicherheit, 11. Aufl. 2023, S. 27.

¹⁶⁶ Eckert, IT-Sicherheit, S. 27.

sensible Daten über einzelne Haushalte vor allem bei der Abholung von Abfall auszuspähen. Ferner wären auch Social-Engineering-Angriffe möglich, indem fremde Personen sich Zutritt zu einer Sortieranlage verschaffen, um dort Innovationen, die durch den Einsatz des ANTs erschaffen wurden, auszuspionieren und ggf. zu verwenden.

Kurzbericht zu technischen Lösungsansätzen

I. Ziel der technischen Lösungsansätze

Im Arbeitspaket 8.1 wurde analysiert, unter welchen Voraussetzungen die sowohl im Projekt als auch in der Anwendung des ANTs erhobenen Daten ausgetauscht und zusammengeführt werden können. Dazu sollten neben rechtlichen Analysen auch technische Lösungsansätze erarbeitet werden, die das Vertrauen der Beteiligten in das Gesamtsystem stärken. In diesem Kurzbericht wird zunächst ein Überblick über die im System vorliegenden Daten und den Schutz, den der ANT in seiner Grundfunktion bereits bietet, dargelegt. Abschließend werden weitergehende technische und organisatorische Schutzmaßnahmen der IT-Sicherheit erläutert, die diesen grundlegenden Schutz des ANTs erweitern und somit einen durchgehenden Schutz im gesamten Systemprozess bieten können.¹⁶⁷

II. Datenverarbeitungen durch den ANT

Der ANT ist ein Konzept zur virtuellen Optimierung eines Geschäftsprozesses parallel zum existierenden, realen Geschäftsprozess. Der Prozess, die verarbeiteten Daten und das Optimierungsziel für den Prozess können für jeden Anwendungsfall passend gewählt werden. Im ANT ist zwischen vier verschiedenen Datenklassen zu unterscheiden: *Materialdaten*, *Sensordaten*, *Verarbeitungsdaten* und *Optimierungsdaten*.

1. Materialdaten

Die *Materialdaten* sind Informationen über die Produkte oder Materialien, die im realen Prozess verarbeitet werden. Im Kontext von *K3I-Cycling* kann es sich dabei etwa um Wertstoffe oder andere Materialien handeln, die für eine neue Verwendung (weiter-)verarbeitet werden. Je nach Anwendungsfall können diese Materialdaten auch personenbezogene Daten beinhalten.

2. Sensordaten

Während des Verarbeitungsprozess erheben die verschiedenen, am Prozess beteiligten Maschinen und Akteure Daten über den laufenden Prozess und den Materialstrom mithilfe von verschiedenen Sensoren (*Sensordaten*). Diese Sensordaten können im ANT mit anderen Beteiligten ausgetauscht werden, um die

¹⁶⁷ Teilergebnisse dieses Berichts wurden veröffentlicht in „Schutz von Geschäftsgeheimnissen in Prozessketten mithilfe eines neuronalen Zwillings“, T. Schneider, B. Steffes und A. Zichler, DuD, Heft 8 2025 (zur Veröffentlichung angenommen).

gemeinsame Verarbeitung des Materials und die Optimierung des Prozesses zu verbessern. Im Kontext von *K3I-Cycling* könnten die Sensoren etwa die Menge oder das Gewicht des verarbeiteten Materials erheben. Je nach Sensor und erhobenen Daten kann es sich bei diesen Daten ebenfalls um personenbezogene Daten handeln.

3. Verarbeitungsdaten

Die *Verarbeitungsdaten* umfassen jene Informationen, die beteiligte Maschinen und Akteure benötigen, um ihren physischen Prozess virtuell im ANT abzubilden und die Verarbeitung somit virtuell zu simulieren. Im Kontext von *K3I-Cycling* könnte es sich dabei um die inneren Arbeitsweisen der prozessbeteiligten Sortieranlagen oder Materialfiltern handeln. Diese Daten können Geschäftsgeheimnisse der jeweiligen Herstellerfirmen sein.

4. Optimierungsdaten

Während der Optimierung des Geschäftsprozesses wird der Einfluss jedes Prozessbeteiligten auf das Optimierungsziel berechnet und diese Informationen (*Optimierungsdaten*) an die jeweiligen zutreffenden Prozessbeteiligten versendet. Im Kontext von *K3I-Cycling* könnte etwa die Laufgeschwindigkeit von Fließbändern einen starken Einfluss auf das Optimierungsziel einer möglichst schnellen Verarbeitung von Material haben.

III. Schutz durch den ANT

Der ANT¹⁶⁸ bietet in seiner grundlegenden Struktur bereits einige Schutzvorkehrungen für die verschiedenen verarbeiteten Datenklassen. So gibt es *keinen Zwang* für die beteiligten Akteure, ihre *Sensordaten mit anderen Prozessteilnehmern zu teilen* und auch die *Verarbeitungsdaten werden nicht an andere Beteiligte weitergeleitet*. Die Verarbeitungslogik bleibt stets auf dem Gerät, auf dem die Verarbeitung virtuell simuliert wird. Hierbei kann es sich um die Maschine selbst handeln (d.h., die Verarbeitungslogik bleibt in der zugehörigen Maschine und somit im Schutzbereich des Maschinenherstellers) oder es kann ein externes Gerät zur Simulation genutzt werden (d.h., die Verarbeitungslogik müsste gegenüber diesem Gerät offengelegt werden). Auch die *Optimierungsdaten*, welche unter Umständen Rückschlüsse auf die Verarbeitungsdaten einer Maschine zulassen können, werden *nur an den jeweiligen Prozessbeteiligten versendet* und gegenüber keinen weiteren Prozessteilnehmern offengelegt.

Einige zentrale Sicherheitsaspekte bleiben jedoch unbeachtet: Der ANT umschreibt nur ein Konzept zur Prozessoptimierung, in dem zwar jeder Prozessteilnehmer nur die Informationen erhält, die er benötigt, es enthält aber keine Maßnahmen zum Schutz gegen das Eingreifen Dritter. Ohne weitere Schutzmaßnahmen könnten sowohl die kommunizierten Daten als auch die in den Maschinen

¹⁶⁸ Die technischen Details finden sich bei: Emmert/Mendez/Dastjerdi/Syben/Maier, The Artificial Neural Twin — Process optimization and continual learning in distributed process chains, Neural Networks 2024, 180, 10664.

gespeicherten Daten von unbeteiligten Dritten abgefangen werden. Ebenfalls denkbar wäre es, dass ein Prozessbeteiligter die ihm im Optimierungsprozess zur Verfügung gestellten Daten nutzt, um Rückschlüsse auf Geschäftsgeheimnisse oder personenbezogene Daten zu ziehen.

IV. Ergänzendes Schutz durch technische und organisatorische Schutzmaßnahmen

Um die im vorangegangenen Kapitel beschriebenen unerlaubten Zugriffe auf die im Prozess verarbeiteten Daten zu unterbinden können unter anderem die hier erläuterten Schutzmaßnahmen genutzt werden.

1. Anonymisierung und Pseudonymisierung

Personenbezogene Daten können durch Anonymisierung oder Pseudonymisierung geschützt werden. Bei einer Pseudonymisierung werden die personenbezogenen Daten in einer Weise verarbeitet, dass sie ohne das Hinzuziehen weiterer Informationen nicht mehr einer spezifischen Person zugeordnet werden können, Art. 4 Nr. 5 DSGVO. Werden personenbezogene Daten anonymisiert, so findet die DSGVO keine Anwendung.¹⁶⁹

Eine Pseudonymisierung der Daten kann beispielweise ein vertrauenswürdiger Dritter durchführen, etwa durch das Ersetzen identifizierender Informationen (wie Namen) durch Pseudonyme. Bekannte Maßnahmen zur Anonymisierung von personenbezogenen Daten sind beispielsweise *k-Anonymität* oder *Differential Privacy*. Das Prinzip von *k-Anonymität* (im Detail bei Samarati et al.¹⁷⁰ zu finden) besagt, dass die identifizierenden Informationen (Quasi-Identifikator) jeder Person derart generalisiert oder zusammengefasst werden sollen, sodass mindestens *k* verschiedene Personen nicht mehr voneinander unterscheidbar sind. Ein System, das *Differential Privacy* (basierend auf Dwork¹⁷¹) ermöglicht, sorgt dafür, dass bei jeder Anfrage an die geschützten Daten nur ein festgelegter Informationsgehalt offengelegt wird. Der Grad des Informationsgehalts wird dabei durch ein leichtes Rauschen angepasst und die Gesamtsumme des offenlegbaren Informationsgehaltes begrenzt.

2. Kommunikationsschutz

Die Kommunikation zwischen den Beteiligten im Prozess sollte vor dem Zugriff Dritter technisch geschützt werden. Zum einen sollten sich die verschiedenen Beteiligten durch geeignete Authentifizierungsmaßnahmen gegenüber den anderen Beteiligten als legitimer Prozess Teilnehmer ausweisen können. Um ein Abhören der Kommunikation zwischen legitimen Prozessbeteiligten zu verhindern, sollte zudem die *gesamte Kommunikation im ANT verschlüsselt* sein. Zur Auswahl eines

¹⁶⁹ Dies ergibt sich aus Erwägungsgrund 26 S. 5, 6 zur DSGVO.

¹⁷⁰ Samarati, P. et al., Protecting privacy when disclosing information: *k*-anonymity and its enforcement through generalization and suppression, Proceedings of the IEEE Symposium on Research in Security and Privacy 1998, Oakland, CA.

¹⁷¹ Dwork, C., Differential privacy, Automata, languages and programming 2006, Springer Berlin Heidelberg.

geeigneten Verfahrens sollte dabei auf aktuelle, *anerkannte Empfehlungen oder Richtlinien* (bspw. von der SOG-IS Crypto Working Group¹⁷²) zurückgegriffen werden.

3. Geräteschutz

Die verschiedenen Datenklassen sollten zudem auch in den Geräten selbst geschützt werden. Zum einen umfasst dies einen Schutz der Daten in den Maschinen, die am physischen Geschäftsprozess beteiligt sind. Diese Maschinen erheben, empfangen und verarbeiten die Daten zur Durchführung des Geschäftsprozesses, als auch der Optimierung. Zudem wird für die Umsetzung des ANTs zusätzlich eine virtuelle Abbildung der Geschäftslogik der jeweiligen Maschinen benötigt – entweder in den besagten Maschinen oder einem weiteren, externen Gerät. In diesem Fall ist auch ein besonderer Schutz der in diesem Gerät vorliegenden Daten und Informationen notwendig.

Um unnötige Angriffsvektoren durch Schnittstellen zu vermeiden (unter anderem empfohlen vom Bundesamt für Sicherheit in der Informationstechnik¹⁷³) sollten alle am Prozess beteiligten Maschinen über nur *jene Schnittstellen verfügen, die sie für den Prozess auch benötigen*. Des Weiteren sollten Maßnahmen ergriffen werden, um das Auslesen von Informationen aus dem Gerät zu verhindern. Dazu könnten etwa Berechnungen in einer *sicheren Laufzeitumgebung* ausgeführt werden, um die Berechnung und Zwischenergebnisse zu schützen, oder auch der gesamte *Speicher des Gerätes verschlüsselt* werden, um gespeicherte Daten und Dateien zu schützen.

4. Organisatorische Schutzmaßnahmen

Ergänzend zu technischen Schutzmaßnahmen sollten zudem auch organisatorische Maßnahmen ergriffen werden. So sollte der *physische Zutritt* zu den am ANT beteiligten Maschinen beschränkt werden, sodass unbeteiligte Dritte keinen Zugriff auf die Hardware der Geräte erhalten. Zudem sollten die Mitarbeiter des Unternehmens, welches den ANT in seinem Prozess einbindet, *Schulungen* erhalten, um konkrete Gefahren für die Datensicherheit durch Dritte im ANT zu erkennen.

Fazit

Der ANT als grundlegendes Konzept zur Optimierung von Unternehmensprozessen bietet bereits einige sehr wichtige technische Mechanismen, durch die personenbezogene Daten und Geschäftsgeheimnisse geschützt werden können. Einige Sicherheitsaspekte werden jedoch durch den ANT nicht beachtet (bspw. das mögliche Abhören der Kommunikation durch Dritte). Diese Aspekte lassen sich durch ergänzende technische und organisatorische Maßnahmen schützen und können somit eine sichere und datenschutzkonforme Anwendung des ANTs in Unternehmen ermöglichen.

¹⁷² Verfügbar unter <https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf>, zuletzt aufgerufen: 01.07.2025, 13.47 Uhr.

¹⁷³ Bundesamt für Sicherheit in der Informationstechnik, *Die Lage der IT-Sicherheit in Deutschland 2023*.