ANONYMISIEREN UND DANN?

Markus Schröder

Markus Schröder, Lehrbeauftragter IT-Recht, Hochschule Heilbronn
Max-Planck-Str. 39, 74081 Heilbronn, DE
markus.schroeder@hs-heilbronn.de; https://www.hs-heilbronn.de

Schlagworte: ***Datenanalysen, Zweckänderung, Löschen, Anonymisieren, Geschäftsgeheimnisschutz***

Abstract: *Bei Verträgen zur Datenanalyse finden sich häufig Klauseln, wonach die überlassenen personenbezogenen Daten nach Beendigung des Auftrags nicht gelöscht bzw. herausgegeben werden müssen. Vielmehr sollen die Daten „nur" anonymisiert werden. Diese Daten werden dann durch den (vormaligen) Auftragnehmer für eigene Zwecke, wie das Anlernen von Algorithmen, genutzt. Nach behördlicher Auffassung kann eine Anonymisierung dem Löschen gleichgestellt werden. Die DS-GVO wäre anschließend nicht mehr anwendbar. Aber es bestehen darüber hinaus noch weitere rechtliche Implikationen.*

1. Einleitung

Unternehmen beauftragen Dienstleister häufig mit Datenanalysen. Dies geschieht, um intern nicht vorhandene Kapazitäten auszugleichen und dennoch neue Informationen, wie Muster oder Regelmäßigkeiten, aus den Daten gewinnen zu können. Von Interesse kann dies insb. im Finanzdienstleitungsbereich sein. In Bereichen, in denen direkte Endkundenbeziehungen bestehen, können diese Datenbestände bzw. Rohdaten auch personenbezogene Daten enthalten. Aus dieser Konstellation resultieren einige datenschutz- und geheimnisschutzrechtliche Herausforderungen. Diese reichen von der Zulässigkeit der Datenanalyse an sich, bis zur Weiterverarbeitung der Daten durch den Dienstleister für eigene Zwecke.

2. Datenschutz – Zweckbindung

Personenbezogene Daten werden im Rahmen von Endkundenbeziehungen regelmäßig nach Art. 6 Abs. 1 lit. b) DS-GVO als für die Durchführung von Vertragsverhältnissen erforderlich erhoben und zunächst hierzu verarbeitet. Nach Auffassung des EDSA ist diese Bestimmung jedoch eng auszulegen. Sie gilt nicht für Situationen, in denen die Verarbeitung für die Erfüllung eines Vertrags nicht wirklich notwendig ist, sondern der betroffenen Person von dem für die Verarbeitung Verantwortlichen einseitig auferlegt wird.[1] Nach dieser engen Auffassung dürften Datenanalysen regelmäßig nicht den eigentlichen Vertragszweck darstellen, der in der Bereitstellung einer Dienstleistung, wie eines Bankkontos oder einer Versicherung, besteht. Es könnte sich bei einer Datenanalyse allerdings um eine nach Art. 6 Abs. 4 DS-GVO zulässige Zweckänderung handeln. Hierbei ist insb. jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung (Art. 6 Abs. 4 lit. a) DS-GVO) sowie der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen (Art. 6 Abs. 4 lit. b) DS-GVO), zu berücksichtigen. Nach Erwägungsgrund 50 Satz 6 sollte der Verantwortliche um festzustellen, ob ein Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, unter anderem prüfen, ob ein Zusammenhang zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken

[1] *EDSA*, Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, Rn. 28.

der beabsichtigten Weiterverarbeitung besteht sowie in welchem Kontext die Daten erhoben wurden, wobei dabei die vernünftigen Erwartungen der betroffenen Personen, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen sind. Nach Erwägungsgrund 47 Satz 3 wiederum ist bei den vernünftigen Erwartungen der betroffenen Person zu prüfen, ob diese zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird.

Die Kontextbezogenheit der vernünftigen Erwartungen ist Grundbestandteil der „Contextual Integrity"-Theorie, die die teilweise extensive Auslegung der „Reasobale Expectation of Privacy-Doctrine" durch-US-Gerichte einzugrenzen versucht. Sie geht aber auch davon aus, dass ein Verantwortlicher, der die durch ihn erhobenen personenbezogenen Daten weiterverarbeitet, den Rahmen des erwartbaren Kontextes regelmäßig nicht verlässt.[2] Ähnliche Maßstäbe legte auch die Art. 29-Datenschutzgruppe bei ihren Ausführungen zum Kompatibilitäts-Assessment an.[3] Da als Zweck der Datenanalyse häufig „Produktverbesserung" o.ä. angegeben wird, kann man hier davon ausgehen, dass der ursprüngliche Kontext der Datenerhebung nicht verlassen wird und die betroffene Person vernünftigerweise diese Datenverarbeitung absehen konnte. Für die Versicherungswirtschaft kann beispielswiese eine Weiterverarbeitung der Daten aus Versicherungsfällen durch ein Versicherungsunternehmen zur Tarifierung und zum Risikomanagement als zulässige Zweckänderung angesehen werden.[4] Nach Erwägungsgrund 50 Satz 2 wäre nun keine gesonderte Rechtsgrundlage für die Weiterverarbeitung erforderlich.[5] Die Weiterverarbeitung ist somit nach Art. 6 Abs. 4 DS-GVO zulässig.[6] Sollte man allerdings mit der Gegenmeinung[7] davon ausgehen, dass im Falle der Weiterverarbeitung eine gesonderte Rechtsgrundlage erforderlich sei, dürften die angeführten Gesichtspunkte im Rahmen der Güterabwägung des Art. 6 Abs. 1 lit. f) DS-GVO ebenfalls regelmäßig zu einer Zulässigkeit der Weiterverarbeitung führen. Es wäre zudem vertretbar, von einer Information der betroffenen Personen nach Art. 13 Abs. 3 und Abs. 4 DS-GVO abzusehen, wenn der Zweck der Datenanalyse bereits in der Information nach Art. 13 Abs. 1 und Abs. 2 DS-GVO benannt wurde.

3. Datenschutz – Löschen

Ist nun die zulässige Datenanalyse durch den Dienstleister durchgeführt und der Auftrag damit beendet worden, müssen die personenbezogenen Daten durch diesen grundsätzlich nach Art. 28 Abs. 3 lit. g) DS-GVO entweder gelöscht oder zurückgegeben werden. An dieser Stelle setzt das eigene Interesse der Dienstleister ein. Diese möchten anonymisierte Datenbestände häufig nach Beendigung der Auftragsverarbeitung weiternutzen, um somit die Datenbasis für das Anlernen ihrer Algorithmen zu vergrößern. Das Löschen der Daten würde diesen Ansatz jedoch unmöglich machen. Daher findet sich in den vertraglichen Regelungen zum Löschen der Daten nach Auftragsbeendigung häufig ein Zusatz wie folgender:

> „*Client acknowledges that the services include pseudonymization and anonymization for the purpose of aggregate reporting and, other than in South Africa, (trends) research, and agrees that Willis Towers Watson may use pseudonymized and anonymized data for its own business purposes, and Willis Towers Watson will comply with all applicable data protection laws in respect of such processing*."[8]

---

2 Nissenbaum, Privacy in Context (2010) S. 233 ff.

3 *Article 29 Working Party*, Opinion 03/2013 on purpose limitation, S. 20 ff.

4 Assion/Nolte/Veil, in: Gierschmann/Schlender/Stentzel/Veil, DS-GVO (2018) Art. 6 Rn. 248.

5 ErwG 50 Satz 2: „In diesem Fall ist keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten.".

6 So auch Raji, DSB 2022, S. 193 (S. 194).

7 Albrecht/Jotzo, Das neue Datenschutzrecht der EU (2017) Teil 3 Rn. 52 ff.

8 Willis Towers Watson Data Processing Protocol – Europe, https://www.wtwco.com/en-gb/notices/data-processing-protocol-europe (zuletzt aufgerufen am 15. Dezember 2023).

Interessant an dieser exemplarischen Vertragsklausel sind die Verweise auf eine Pseudo- und eine Anonymisierung. Eine Pseudonymisierung der Daten wäre zwar bei der Zulässigkeit einer Weiterverarbeitung nach Art. 6 Abs. 4 lit. e) DS-GVO zu berücksichtigen und wäre nach den Erwägungsgründen 28 und 75 risikomindernd. Dennoch wären die Daten nach Art. 4 Nr. 1 DS-GVO noch personenbezogen, so dass eine Weiterarbeitung dieser Daten durch den Auftragsverarbeiter für eigene Zwecke ausscheidet oder nach Art. 28 Abs. 10 DS-GVO den Anforderungen an einen Verantwortlichen i.S.v. Art. 4 Nr. 7 DS-GVO entsprechen müsste, wie insb. eigenen Informationspflichten nach Art. 14 DS-GVO. Zudem dürfte sich durch die vertragliche Zusicherung an den Dienstleister, pseudonymisierte Daten für eigene Zwecke weiterverarbeiten zu dürfen, die nichtdispositive Pflicht zur Löschung bzw. Herausgabe personenbezogener Daten nach Auftragsbeendigung aus Art. 28 Abs. 3 lit. g) DS-GVO nicht umgehen lassen. Relevanter ist daher der Verweis auf die Weiterverarbeitung anonymisierter Daten. Art. 28 Abs. 3 lit. g) DS-GVO spricht ausdrücklich davon, dass die Daten nach Auftragsbeendigung durch den Auftragsverarbeiter gelöscht oder zurückgegeben werden müssen. Allerdings hat die österreichische Datenschutzbehörde im Falle einer Versicherung entschieden, dass die Anonymisierung der Daten einem Löschen gleichzustellen ist.[9] Hierbei wurden die Daten aus der ursprünglichen Kundenverbindung mit einer „Dummy Kundenverbindung" überschrieben.[10] Diese Auffassung ist rechtlich überzeugend, da die DS-GVO nach Art. 2 Abs. 1 und Erwägungsgrund 26 nur auf die Verarbeitung personenbezogener Daten Anwendung findet, so dass dies gerade bei anonymen Daten nicht der Fall ist und diese Möglichkeit demnach nicht ausdrücklich in Art. 28 Abs. 3 lit. g) DS-GVO erwähnt werden muss.

Nach vereinzelt vertretener behördlicher Auffassung verlangt eine Anonymisierung allerdings in jedem Falle die Durchführung einer Datenschutz-Folgenabschätzung.[11] So begründete der deutsche Bundesbeauftragte für Datenschutz und Informationsfreiheit dies damit, dass es sich bei einer Anonymisierung regelmäßig um einen umfangreichen Verarbeitungsvorgang handelt und bei einer Anonymisierung regelmäßig in großem Umfang eine neue Technologie eingesetzt würde. Diese Argumentation knüpft zwar an die Fälle der Erforderlichkeit einer Datenschutz-Folgenabschätzung nach Erwägungsgrund 91 Satz 1 an. Sie vermag dennoch nicht zu überzeugen, da diese Voraussetzungen im Einzelfall zwar vorliegen können, aber eben immer einer Einzelfallbewertung bedürfen. Gleichwohl bietet es sich in den hier behandelten Fällen an, eine Datenschutz-Folgenabschätzung durchzuführen. So kann auch durch eine freiwillige Datenschutz-Folgenabschätzung dem Vorwurf entgangen werden, eine etwaig verpflichtende Datenschutz-Folgenabschätzung sei nicht durchgeführt worden.[12] Nimmt man hier ein hohes Risiko für die betroffenen Personen an, liegt dieses allerdings nicht in den einzelnen Fällen vor, die sich exemplarisch in Art. 35 Abs. 3 DS-GVO und in Erwägungsgrund 91 finden. Vielmehr liegt das Risiko gerade darin, dass auf anonymisierte Daten die DS-GVO nach deren Art. 2 Abs. 1 keine Anwendung mehr findet, so dass die Daten ohne die Restriktionen des Zweckbindungs- und des Datenminimierungsgrundsatzes[13] weiterverarbeitet werden dürften. Zudem wird in Erwägungsgrund 75 die unbefugte Aufhebung der Pseudonymisierung als Risiko für die Rechte und Freiheiten natürlicher Personen angeführt. Nichts anderes kann für eine unbefugte Aufhebung der Anonymisierung gelten. Zudem würden die betroffenen Personen im Falle einer Re-Identifizierung i.S.v. Erwägungsgrund 75 daran gehindert, die sie betreffenden personenbezogenen Daten zu kontrollieren.[14] Diese Risiken erhöhen sich durch eine Weiterverarbeitung der anonymisierten Daten kontinuierlich.[15]

9 *DSB*, GZ: DSB-D123.270/0009-DSB/2018 v. 05.12.2018.
10 *DSB*, GZ: DSB-D123.270/0009-DSB/2018 v. 05.12.2018, Ziff. A.4.7).
11 *BfDI*, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, Stand: 29. Juni 2020, S. 11; *ICO*, Anonymisation: managing data protection risk code of practice, November 2012, S.40 f.
12 Franke, RDi 2023, S. 565 (S. 570).
13 Art. 5 Abs. 1 lit. b) und lit. c) DS-GVO.
14 Pohle/Hölzel, Anonymisierung aus Sicht des Datenschutzes und des Datenschutzrechts, S.6.
15 Rossnagel, ZD 2021, S. 188 (S. 191).

Da durch die Anonymisierung der Daten eine Veränderung der Risikosituation eintritt, wird auch in der Literatur teilweise die Durchführung einer Datenschutz-Folgenabschätzung verlangt.[16] Man kann hier somit aus den genannten Gründen durchaus ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen annehmen. Zwar dürfte auch durch eine entsprechende Datenschutz-Folgenabschätzung das Risiko einer unbefugten Aufhebung der Anonymisierung nicht gänzlich ausgeschlossen werden können. Hier greift jedoch der risikobasierte Personenbezug, der sich in der europäischen Rechtsprechung etabliert hat. Demnach liegt kein Personenbezug vor, wenn die Identifizierung der betreffenden Person gesetzlich verboten oder praktisch nicht durchführbar wäre, z. B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, so dass das Risiko einer Identifizierung de facto vernachlässigbar erscheint.[17] Ist die Pseudonymisierung jedenfalls schon risikomindernd, kann sie somit allerdings auch eine anonymisierende Wirkung entfalten.[18] Eine Datenschutz-Folgenabschätzung ist zwar grundsätzlich nach Art. 35 Abs. 1 DS-GVO vom Verantwortlichen selbst durchzuführen. Allerdings muss der Auftragsverarbeiter diesen nach Art. 28 Abs. 3 lit. f) DS-GVO bei deren Durchführung unter Berücksichtigung der ihm zur Verfügung stehenden Informationen unterstützen. Da die Löschung und damit auch die dieser datenschutzrechtlich gleichgestellte Anonymisierung nach Art. 28 Abs. 3 lit. g) DS-GVO vom Auftragsverarbeiter durchzuführen ist, verfügt auch nur dieser über die Informationen zur eingesetzten Anonymisierungstechnik. Daher muss er diese Informationen, ähnlich einem „klassischen" Löschnachweis, dem Verantwortlichen zur Durchführung der Datenschutz-Folgenabschätzung zur Verfügung stellen. Bei Erfüllung der genannten Anforderungen wäre eine Weiterverarbeitung der anonymisierten Daten durch den (vormaligen) Auftragsverarbeiter für eigene Zwecke datenschutzrechtlich möglich.

4. Geschäftsgeheimnisschutz

Aber auch, wenn der sachliche Anwendungsbereich der DS-GVO nach deren Art. 2 Abs. 1 verlassen wird, stellen sich dennoch weitere Rechtsfragen. So könnte der Auftraggeber durch eine vertragliche Zusicherung wie die obige seinen Geschäftsgeheimnisschutz verlieren. Nach § 2 Nr. 1 lit. a) GeschGehG bzw. § 26b Abs. 1 Nr. 1 und 2 öUWG ist ein Geschäftsgeheimnis eine Information, die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem bzw. kommerziellem Wert ist. Nach der herrschenden Meinung sind hiervon auch Rohdaten und sog. Datenpools umfasst.[19] So werden aus den Rohdaten weitergehende Informationen gewonnen oder entwickelt, so dass ein Schutz bereits auf dieser vorgelagerten Ebene ansetzen muss.[20] Nach § 2 Nr. 1 lit. b) GeschGehG bzw. § 26b Abs. 1 Nr. 3 öUWG müssen diese Geschäftsgeheimnisse jedoch auch Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber sein. Es stellt sich somit die Frage, ob in Fällen, in denen der Inhaber dieser Geschäftsgeheimnisse diese durch eine vertragliche Zusicherung einem Dritten offenbart, noch angemessene Geheimhaltungsmaßnahmen vorliegen. Diese Maßnahmen können vertraglicher und technischer Natur sein. Aus vertraglicher Sicht bietet es sich an, zusätzlich zur Vereinbarung über die Auftragsverarbeitung eine Geheimnisschutzvereinbarung (sog. NDA)

[16] Rossnagel, ZD 2021, S. 188 (S. 191 f.); Pohle/Hölzel, Anonymisierung aus Sicht des Datenschutzes und des Datenschutzrechts, S. 5 f.

[17] EuGH 9. November 2023, C-319/22, Rn. 45; EuGH 19. Oktober 2016, C-582/14, Rn. 46; EuG 26. April 2023, T-557/20, Rn. 93; s. hierzu Seidel, DSB 2023, S. 212 ff.; Fischer, DSB 2023, S. 215 ff.; Johannes, RDV 2023, S. 254 ff.; Baumgartner, ZD 2023, S. 399 ff.; zum risikobasierten Personenbezug s. auch Schmitz, ZD 2018, S. 5 (S. 8).

[18] Rossnagel, ZD 2018, S. 243 (S. 246): „Anonymisierende Pseudonymisierung".

[19] Hacker, GRUR 2020, S. 1025 (S. 1032); Hauck, NJW 2016, S. 2218 (S. 2221); ders.: in Münchener Kommentar zum Lauterkeitsrecht, § 2 GeschGehG Rn. 5; Keller, in: Keller/Schönknecht/Glinke, Geschäftsgeheimnisschutzgesetz, § 2 Rn. 41 ff.; Krüger/Wiencke/Koch, GRUR 2020, S. 578 ff.; Ohly, GRUR 2019, S. 441 (S. 443); ders, in: Ohly/Sosnitza, Gesetz gegen den unlauteren Wettbewerb, § 2 GeschGehG Rn. 3.

[20] Hauck, NJW 2016, S. 2218 (S. 2221).

zu schließen.[21] Zunächst ist hier zu berücksichtigen, dass eine allgemein formulierte Vereinbarung zur Gewährleistung des Schutzes nach dem GeschGehG bzw. den §§ 26a ff. öUWG nicht ausreicht. Insbesondere ist aufzuführen, welche Informationen Geschäftsgeheimnisse sind.[22]

Doch auch bei einer konkret gestalteten Geheimnisschutzvereinbarung verbleibt für den Geheimnisinhaber das Risiko eines dauerhaften Verlustes des Geheimnisschutzes durch den Wegfall der Geheimnisqualität, da trotz Vorliegen einer Geheimnisschutzvereinbarung die überlassenen Daten für Dritte zugänglich sein könnten.[23] Dies würde zwar regelmäßig nicht für die Rohdaten selbst gelten. Aber dennoch werden durch die Dienstleister die u.a. mit diesen Daten trainierten Algorithmen auch anderen Kunden im Rahmen von KI-Lösungen angeboten. Hier verbleibt für das überlassende Unternehmen zumindest die Rechtsunsicherheit, ob dies gleichzeitig zum Verlust des Geheimnisschutzes an den zugrundeliegenden Rohdaten führt. Auch ist es fraglich, ob Geheimhaltungsmaßnahmen angemessen i.S.v. § 2 Nr. 1 lit. b) GeschGehG bzw. § 26b Abs. 1 Nr. 3 öUWG sind, die lediglich vertraglichem, nicht aber technischem Schutz unterliegen.[24] Zunächst spricht für das Vorliegen geeigneter technischer Schutzmaßnahmen, dass der Dienstleister bereits bei Abschluss der Vereinbarung zur Auftragsverarbeitung nach Art. 28 Abs. 3 lit. c) i.V.m. § 32 DS-GVO geeignete technische und organisatorische Maßnahmen treffen muss. Zwar besteht hierzu nach Auftragsbeendigung keine Verpflichtung gegenüber dem vormaligen Auftraggeber mehr. Dennoch wird der Dienstleister regelmäßig diese Maßnahmen grundsätzlich und von einem spezifischen Auftrag losgelöst entsprechend implementiert haben. Im Rahmen § 2 Nr. 1 lit. b) GeschGehG bzw. § 26b Abs. 1 Nr. 3 öUWG wird als technische Schutzmaßnahme bei Daten regelmäßig eine Zugangssicherung durch Verschlüsselungstechniken, Passwörter und dergleichen verlangt.[25] Auch wird die Umsetzung des sog. „need-to-know-Prinzips“ verlangt, wonach nur solche Mitarbeiter Zugang zu gesicherten Räumen, Unterlagen und Daten erhalten, die die entsprechende Information für ihre Arbeit benötigen.[26] Diese Maßnahmen finden aus datenschutzrechtlicher Sicht ihre Entsprechung in Art. 32 Abs. 1 lit. a) und b) DS-GVO. Theoretisch können diese Maßnahmen geeignet sein, ein öffentliches Verfügbarmachen i.S.d. § 3 Abs. 1 Nr. 2 lit. a) GeschGehG bzw. § 26d Abs. 2 Nr. 2 öUWG zu verhindern. In der Praxis stellt sich jedoch die Frage, ob ein weiterverarbeitender Dienstleister bereit ist, diese Maßnahmen in Gänze vertraglich zuzusichern, da er nach Auftragsbeendigung jedenfalls von der direkten vertraglich nicht dispositiven Verpflichtung nach Art. 28 Abs. 3 lit. c) i.V.m. § 32 DS-GVO befreit ist und daher diese vertragliche Verpflichtung aus seiner Sicht überobligatorisch wäre. Weiterhin könnte bei einer strengen Ausgestaltung dieser Maßnahmen die Datennutzung für eigene Zwecke zumindest erschwert werden. So dürfte eine Verschlüsselung regelmäßig schwierig, das need-to-know-Prinzip, jedenfalls bezogen auf die Rohdaten, besser in einer Geheimnisschutzvereinbarung abbildbar sein. Zu bedenken ist jedoch auch, dass diese Vereinbarungen in der Praxis meist zeitlich begrenzt sind. Zu denken ist hier an eine Befristung auf fünf Jahre, da nach der Rechtsprechung davon auszugehen ist, dass Geschäftsgeheimnisse nach einem Zeitraum von fünf Jahren typischerweise nicht mehr aktuell und deshalb nicht mehr vertraulich sind.[27]

Aber auch bei Abschluss einer wirksamen Geheimnisschutzvereinbarung verbleibt ein Spannungsverhältnis zu Rechten, die der Dienstleister etwaig selbst an den erhaltenen Daten erlangen könnte. Diskutiert wird hier insbesondere ein Recht des Datenbankherstellers nach den §§ 87a ff. UrhG bzw. §§ 76c ff. öUrhG. Ob die Tatbestandsmerkmale, die zu diesem sui generis-Recht führen, erfüllt wären, ist jedoch noch umstritten. Insbesondere ist unklar, wie genau die hinreichende Wesentlichkeit der für den Leistungsschutz erforderlichen Investition in die Datenbank festzustellen ist. Häufig sind die Angebote von Dienstleistern, die sich die

21 Grundsätzlich zu Datenlizenzverträgen s. Hennemann, RDi 2021, S. 61 ff.
22 ArbG Aachen 13. Januar 2022, 8 Ca 1229/20.
23 Bussmann/Glasowski/Niehaus/Stecher, RDi 2022, S. 391 (S. 394).
24 Krüger/Wiencke/Koch, GRUR 2020, S. 578 (S. 582).
25 Alexander, in: Köhler/Bornkamm/Feddersen, Gesetz gegen den unlauteren Wettbewerb, § 2 GeschGehG Rn. 63.
26 Keller, in: Keller/Schönknecht/Glinke, Geschäftsgeheimnisschutzgesetz, § 2 Rn. 64.
27 EuGH 19. Juni 2018, C-15/16, Rn. 54; BVerwG 30. Januar 2020, 10 C 18.19, Rn. 16.

Weiterverarbeitung der überlassenen Daten vorbehalten, günstiger als vergleichbare Angebote ohne diesen Vorbehalt. Fraglich ist aber, ab welchem Schwellenwert diese Rabattierung als wesentliche Investition und damit als den Leistungsschutz begründend anzusehen wäre. Annehmen könnte man dies jedenfalls, wenn die Erbringung der Dienstleitung für den Auftragnehmer nicht mehr oder nur kostendeckend wäre. Zwar ist der Aufwand für die Erzeugung der in der Datenbank enthaltenen Daten nicht allein maßgeblich, da im Laufe des Trainingsprozesses die eingespeisten Daten angereichert und in diesem Sinne erst erzeugt werden. Allerdings ist die Abgrenzung zwischen dem hierfür anfallenden, nicht maßgeblichen Aufwand und dem berücksichtigungsfähigen Aufwand für die Beschaffung, Überprüfung oder Darstellung der in der Datenbank enthaltenen Daten in diesem Fall mit Unsicherheiten belastet.[28] Daher besteht aus Sicht des überlassenden Unternehmens das Risiko, dass der Dienstleister ein solches Recht für sich in Anspruch nehmen könnte. Dieses Recht schützt allerdings nicht die in der Datenbank enthaltenen Daten selbst, sondern nur die in die Datenbank Investierenden vor unberechtigter Vervielfältigung, Verbreitung oder öffentlicher Zugänglichmachung eines wesentlichen Teils der Datenbank, so dass dieses Investitionsschutzrecht auch aus Sicht der Dienstleister keine Rechtssicherheit bei der Verwertung von überlassenen Trainingsdatensätzen bietet.[29]

5. Fazit

Für Unternehmen ist es sehr interessant, aus ihren Datenbeständen lernen und neue Erkenntnisse gewinnen zu können. Sind die entsprechenden Kapazitäten intern nicht vorhanden, stehen zahlreiche Dienstleister zur Verfügung, die dies übernehmen können und wollen. Häufig lassen sich diese jedoch vertraglich zusichern, diese Daten nach Auftragsbeendigung für eigene Analyse- und Trainingszwecke weiternutzen zu dürfen. Datenschutzrechtlich kann man Rechtsrisiken hier mit einer Anonymisierung begegnen, wobei der Dienstleister dem Auftraggeber Informationen zur Wirksamkeit der Anonymisierung zur Verfügung stellen müsste. Danach bestehen aber weiterhin erhebliche Risiken für das die Daten überlassende Unternehmen im Bereich des Geheimnisschutzes. Zwar kann man hier bestehende Risiken durch den Abschluss einer Geheimnisschutzvereinbarung und die Vereinbarung zusätzlicher technischer Schutzmaßnahmen minimieren. Aber eben nur minimieren, nicht jedoch ausschließen. Daher muss bis auf Weiteres jedes Unternehmen im Einzelfall für sich entscheiden, ob der wirtschaftliche Wert der Datenanalyse oder der drohende Verlust des Geheimnisschutzes bei der Risikoabwägung überwiegt. Es bleibt abzuwarten, ob beim Geheimnisschutz für Trainingsdaten weiterer gesetzlicher Regelungsbedarf erkannt und umgesetzt werden wird.[30]

So wird anlässlich einer Studie für die Europäische Kommission zum Geheimnisschutz in der Datenökonomie diskutiert, dass in die Erwägungsgründe zur Geschäftsgeheimnisrichtlinie[31] eine Klarstellung aufgenommen werden sollte, wonach Rohdaten keine Geschäftsgeheimnisse darstellen können.[32] Dies würde sich auf der einen Seite zwar in Regelungen, wie den Data Act[33] einfügen, die ein Datenteilen vereinfachen sollen. Auf der anderen Seite würde dies aber gleichzeitig faktisch dessen auf maschinengenerierte Daten begrenzten Anwendungsbereich[34] in den Regelungsbereich der Geschäftsgeheimnisrichtlinie hinein erweitern. Zudem sind auch nach dem Data Act Geschäftsgeheimnisse bei der Offenlegung durch den Dateninhaber an einen

[28] Apel/Kaulartz, RDi 2020, S. 24 (S. 28).
[29] Bussmann/Glasowski/Niehaus/Steche, RDi 2022, S. 391 (S. 395).
[30] S. hierzu Bartke/Hoffmann/Skiebe, RDi 2022, S. 431 ff.
[31] 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
[32] Aplin/Radauer/Bader/Searle, IIC 2023, S. 826 (S. 854).
[33] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz); grundsätzlich zu einem vereinfachten Datenzugang s. Ramge/Mayer-Schönberger, Machtmaschinen (2020) S. 100 ff.; dies., Das Digital, (2017) S. 245 ff.
[34] Erwägungsgrund 14 Data Act.

Nutzer[35] sowie bei einer Offenlegung durch den Nutzer an einen Dritten jeweils durch „besonderen Maßnahmen“ zu schützen.[36] Allerdings geht der angeführte Regelungsvorschlag zu den Erwägungsgründen der Geschäftsgeheimnisrichtlinie sogar noch darüber hinaus und würde zu einer uneinheitlichen Berücksichtigung des Geschäftsgeheimnisschutzes in vergleichbaren Bereichen führen. Für maschinengenerierte Daten würde der Geschäftsgeheimnisschutz gelten, für sonstige Daten jedoch nicht. Zwar könnte hierdurch Rechtssicherheit isoliert für den Bereich der Weiterverarbeitung anonymisierter Daten durch einen Dienstleister außerhalb des Anwendungsbereichs des Data Act eintreten. Jedoch wären diese Regelungen inkonsistent und die hier beschriebenen Geschäftsmodelle gerade dadurch gefährdet. So hätten Datenanalyseunternehmen künftig wahrscheinlich weniger Möglichkeiten Trainingsdaten zu generieren. Auftraggeber dürften weniger Datenanalysen extern durchführen lassen, um die Geschäftsgeheimniseigenschaft ihrer Rohdaten nicht zu verlieren.

6. Literatur

Albrecht, Jan Philipp/Jotzo, Florian: Das neue Datenschutzrecht der EU, 1. Aufl., Baden-Baden 2017.

Apel, Simon/Kaulartz, Markus: Rechtlicher Schutz von Machine Learning-Modellen, RDi 2022, S. 24–34.

Bartke, Lukas/Hoffmann Kira-Sophie: Der Schutz von Trainingsdaten de lege ferenda – What would Machlup do?, RDi 2022, S. 431–438.

Baumgartner, Ulrich: Bestimmung des Personenbezugs von Daten, ZD 2023, S. 399–404.

Bussmann, Sarah/Glasowski, Carolin/Niehaus, Michael/Stecher, Sarah: Die Schutzfä-higkeit von KI-Trainingsdaten de lege lata – What would Machlup find?, RDi 2022, S. 391–396.

Fischer, Celin: EuG zum Begriff der personenbezogenen Daten: Schon anonymisierte oder noch pseudonymisierte Daten?, DSB 2023, S. 215–219.

Franke, Lucia: Datenschutzrechtskonformes Training von KI-Systemen mit öffentlich verfügbaren personenbezogenen Daten, RDi 2023, S. 565–571.

Gierschmann, Sibylle/Schlender, Katharina/Stentzel, Rainer/Veil, Winfried: Kommentar Datenschutz-Grundverordnung, 1. Aufl., Köln 2018.

Hacker, Philipp: Immaterialgüterrechtlicher Schutz von KI-Trainingsdaten, GRUR 2020, S. 1025–1033.

Hauck, Ronny: Geheimnisschutz im Zivilprozess – was bringt die neue EU-Richtlinie für das deutsche Recht?, NJW 2016, S. 2218–2223.

Heermann, Peter W./Schlingloff, Jochen (Hrsg.): Münchener Kommentar zum Lauterkeitsrecht, 3. Aufl., München 2022.

Hennemann, Moritz: Datenlizenzverträge, RDi, S. 61–70.

Johannes, Paul C.: Kein Personenbezug bei fehlenden Mitteln des Datenempfängers zur Re-Identifizierung, RDV 2023, S. 254–257.

Keller, Erhard/Schönknecht, Marcus/Glinke, Anna: Geschäftsgeheimnisschutzgesetz, 1. Aufl., München 2021.

Köhler, Helmut/Bornkamm, Joachim/Feddersen, Jörn: Gesetz gegen den unlauteren Wettbewerb, 41. Aufl. München 2023.

Krüger, Stefan/Wiencke, Julia/Koch, André: Der Datenpool als Geschäftsgeheimnis, GRUR 2020, S. 578–584.

Mayer-Schönberger, Viktor/Ramge, Thomas: Das Digital – Markt, Wertschöpfung und Gerechtigkeit im Datenkapitalismus, 1. Aufl., Berlin 2017.

Nissenbaum, Helen: Privacy in Context – Technology, Policy, and the Integrity of Social Life, 1. Aufl., Stanford 2010.

Ohly, Ansgar: Das neue Geschäftsgeheimnisgesetz im Überblick, GRUR 2019, S. 441–451.

Ohly, Ansgar/Sosnitza, Olaf: Gesetz gegen den unlauteren Wettbewerb, 8. Aufl, München 2023.

Paal, Boris/Fenik, Maroš: Access to Data in the Data Act Proposal, ZfDR 2023, S. 249–262.

[35] Art. 4 Abs. 3 Data Act.

[36] Art. 5 Abs. 8 Data Act; s. hierzu Wiebe, GRUR 2023, S. 227 (S. 232 ff.); Paal/Fenik, ZfDR 2023, S. 249 (S. 258).

Pohle, Jörg/Hölzel, Julian: Anonymisierung aus Sicht des Datenschutzes und des Datenschutzrechts – Stellungnahme zum Konsultationsverfahren des BfDI zur Anonymisierung unter der DS-GVO unter besonderer Berücksichtigung der TK-Branche, aufrufbar unter https://www.hiig.de/wp-content/uploads/2020/03/2020-Pohle-H%C3%B6lzel-Anonymisierung-aus-Sicht-des-Datenschutzes-und-des-Datenschutzrechts.pdf (zuletzt aufgerufen am 15. Dezember 2023).

Raji, Behrang: Privilegiertes Training von KI-Systemen, DSB 2022, S. 193–195.

Ramge, Thomas/Mayer-Schönberger, Viktor: Machtmaschinen – Warum Datenmonopole unsere Zukunft gefährden und wie wir sie brechen, 1. Aufl., Hamburg 2020.

Rossnagel, Alexander: Pseudonymisierung personenbezogener Daten – Ein zentrales Instrument im Datenschutz nach der DS-GVO, ZD 2018, S. 243–247.

Rossnagel, Alexander: Datenlöschung und Anonymisierung – Verhältnis der beiden Datenschutzinstrumente nach DS-GVO, ZD 2021, S. 188–192.

Schmitz, Barbara: Der Abschied von Personenbezug – Warum der Personenbezug nach der DS-GVO nicht mehr zeitgemäß ist, ZD 2018, S. 5–8.

Seidel, Hendrik: Der Personenbezug von Daten ist (weiterhin) relativ zu bestimmen – das EuG erinnert an „Breyer“, DSB 2023, S. 212–214.

Wiebe, Andreas: The Data Act Proposal – Access rights at the Intersection with Database Rights and Trade Secret Protection, GRUR 2023, S. 227–238.

Zech, Herbert: „Industrie 4.0“ – Rechtsrahmen für eine Digitalwirtschaft im digitalen Binnenmarkt, GRUR 2015, S. 1151–1160.