Digitaler Aktionsplan Smart Farming

Rechtswissenschaftliche Bewertung

Die Studie erfolgte im Rahmen des Strategieprozesses „Smart Farming" des Digitalen Aktionsplans Austria im Auftrag des Bundesministeriums für Finanzen.

Impressum

Universität für Weiterbildung Krems
Department für Rechtswissenschaften
und internationale Beziehungen
Zentrum für Geistiges Eigentum, Medien-
und Innovationsrecht

Dr.-Karl-Dorrek-Straße 30
A-3500 Krems an der Donau
Tel.: +43 2732 893
Fax.: +43 2732 893

www.donau-uni.ac.at/ipcenter

Stand: 5. 9. 2023

Inhaltsverzeichnis

Inhaltsverzeichnis 3
Begleitende rechtswissenschaftliche Analyse des Rechtsrahmens für einen Agriculture Data Space 4
Leitszenario 4
Faktische und rechtliche Allokation von landwirtschaftlichen Daten und Informationen 6
Zugangsrechte zu Daten und Information 21
Umfang einer rechtlich zulässigen Verwertung 30
Zusammenfassende Rahmenbedingungen eines Data Spaces „Smart Farming" 33
Handlungsempfehlungen und -spielräume 35
Anhang: Verzeichnisse 36
Abkürzungsverzeichnis 36
Abbildungsverzeichnis 36

Begleitende rechtswissenschaftliche Analyse des Rechtsrahmens für einen Agriculture Data Space

Die Erzeugung, Sammlung, Verarbeitung und Verwertung von landwirtschaftlich relevanten Daten eröffnet entlang des geltenden österreichischen Rechts sowie der Digital-Rechtsakte der Europäischen Union zahlreiche rechtliche Aspekte. Gegenstand der nachfolgenden Untersuchung sind die aktuellen und absehbaren rechtlichen Rahmenbedingungen für die Schaffung eines effektiven und effizienten Ökosystems für die Nutzung land- und forstwirtschaftlicher Daten. Die Untersuchung zeigt schließlich Handlungsempfehlungen und -spielräume auf, die auf individueller (betrieblicher) Ebene oder Verwaltungsebene sowie auf gesetzgeberischer Ebene bestehen. Ausgangspunkt bildet ein abstraktes Szenario, das paradigmatische Fragestellungen illustriert.

Leitszenario

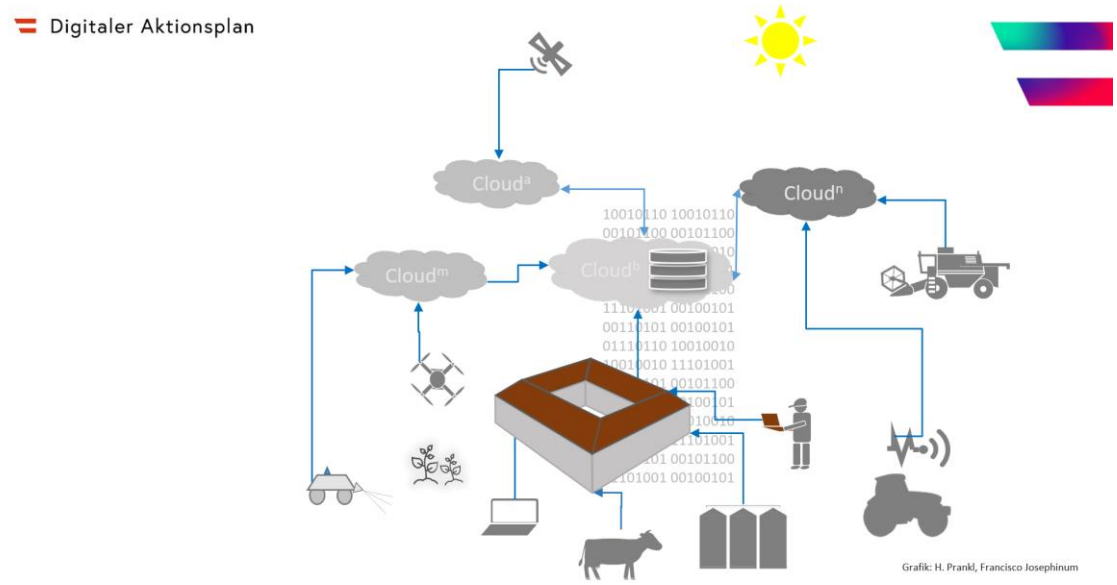

Abbildung 1: Exemplarisches Szenario – Akteure und Interaktion

Akteure

- Landwirtschaftlicher Betrieb
- Abnehmerinnen und Abnehmer landwirtschaftlicher Produkte
- Landmaschinenherstellerinnen / Landmaschinenhersteller (und deren Zuliefererinnen und Zulieferer)
- Landmaschinen-Dienstleisterinnen bzw. - Dienstleister
- Landmaschinen-Verleiherinnen bzw. - Verleiher
- Intermediäre (zB Farm Management System Anbieter)
- kommerzielle Datennutzer (zB Versicherungen, Saatguthersteller etc)
- nicht-kommerzielle Datennutzer (zB wissenschaftliche Forschung)
- öffentliche Verwaltung (Bund, Länder und Gemeinden)
- externe Datenquellen

Typischer Sachverhalt

Der landwirtschaftliche Betrieb *LW* umfasst Pflanzenproduktion und Tierhaltung. Die betrieblichen Daten werden im Farm-Management-Informationssystem des Herstellers *FMS* erfasst und verwaltet sowie in dessen zentraler Cloud gespeichert. *LW* nutzt zudem verschiedene externe Datenquellen, zB Wetterdaten, zur Planung betrieblicher Vorgänge. Schließlich hat *LW* ausführliche innerbetriebliche Dokumentationen über Bodennutzung, Tierhaltung und Vermarktung. FMS verfügt über die Betriebsdaten unterschiedlicher landwirtschaftlicher Betriebe.

LW setzt verschiedene smarte Landmaschinen der Herstellerin bzw. des Herstellers *LMH* ein, die zahlreiche Nutzungs- und Sensordaten sammeln. Die Landmaschinen sind teilweise Eigentum von *LW*, teilweise werden aber auch Landmaschinen-Dienstleisterinnen bzw. -Dienstleister (zB Erntemaschinen) beigezogen, die ihrerseits smarte Landmaschinen einsetzen und Daten erzeugen sowie sammeln. Unter Umständen werden Landmaschinen auch gemeinschaftlich von mehreren Betrieben angeschafft und genutzt oder über Landmaschinen-Verleiher LMV angemietet. Auch das Nutzvieh ist mit smarten Sensoren ausgestattet, die etwa Standort und Gesundheitsdaten der Tiere erheben. Diese Daten sind *LW* allerdings nur beschränkt und innerhalb proprietärer Softwareumgebungen der Herstellerin bzw. des Herstellers zugänglich.

LW hat ein Interesse an der Teilhabe an einem gemeinschaftlichen Datenraum, will aber zugleich die Hoheit über „eigene“ Daten behalten und ihre Nutzung nachvollziehen können.

Variante 1: *LW* will Landmaschinendaten und/oder Tiersensordaten zur Verbesserung betrieblicher Vorgänge nutzen. Dabei sollen ggf. auch weitere externe Datenquellen einbezogen werden

Variante 2: *LMH* will Landmaschinendaten zur Produktentwicklung nutzen.

Variante 3: *Versicherungsunternehmen* will Landmaschinendaten, landwirtschaftliche Betriebsdaten etc zur Ausgestaltung von (neuen) Versicherungsprodukten verwenden.

Variante 4: *Länder/Gemeinden* wollen Daten über Bewirtschaftung und Bodennutzung landwirtschaftlicher Flächen für Zwecke der Raumplanung verwerten.

Variante 5: *Forschungseinrichtungen* wollen landwirtschaftliche Daten aus verschiedenen Quellen für nicht-kommerzielle Forschungsvorhaben nutzen.

Variante 6: Im Förderwesen sowie im Rahmen gesetzlicher Informations- und Offenlegungspflichten sind landwirtschaftlichen Daten an die öffentliche Verwaltung zu übermitteln. In der Folge sollen diese Daten für andere Verwaltungszwecke und statistische Zwecke genutzt werden.

Variante 7: Nutzung von Daten der öffentlichen Verwaltung im Sinne von Open Government Data für privatwirtschaftliche Zwecke.

Leitende Fragestellungen

Der Untersuchung liegen mit Blick auf die Erzeugung, Sammlung, Verarbeitung und Verwertung landwirtschaftlicher Daten (insbesondere Maschinendaten, Tiersensordaten oder betriebliche Daten) folgenden leitende Fragestellungen zu Grunde:

- **Wem „gehören“ landwirtschaftliche Daten?**
- **Wer hat unter welchen Umständen Zugangsrechte zu landwirtschaftlichen Daten?**
- **Wer darf unter welchen Umständen landwirtschaftliche Daten verwerten?**

Faktische und rechtliche Allokation von landwirtschaftlichen Daten und Informationen

Ausgangspunkt der rechtlichen Analyse ist die Frage der rechtlichen Allokation von landwirtschaftlichen Daten (Landmaschinendaten, Viehdaten und landwirtschaftlich-betriebliche Daten). Von der rechtlichen Allokation ist die faktische zunächst zu unterscheiden: In letzterer Hinsicht sind diese Daten denjenigen zuzuordnen, die faktische Herrschaft („Kontrolle") darüber haben. Faktische Herrschaft („Haben") ist nicht notwendig ein Indiz für die rechtliche Zuordnung dieser Daten („Haben dürfen").

Der nachfolgenden rechtswissenschaftlichen Untersuchung wird folgendes Verständnis des Begriffspaars „Daten" und Information zu Grunde gelegt:

Als **Daten** sind die „*digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material*"[1] zu verstehen. Daten sind demnach als digitale Informationsträger zu verstehen, wenn sie als „Darstellung" von Information definiert sind. Auch in der einschlägigen technischen Norm werden Daten als „*wiederinterpretierbare Darstellung von Informationen in einer formalisierten und zur Kommunikation, Interpretation oder Verarbeitung geeigneten Form*"[2] verstanden. Der Datenbegriff des DGA (und des erwarteten EU Data Acts) sowie der einschlägigen Normen setzt – semiotisch betrachtet – auf der Syntaxebene an, die insofern von der inhaltlichen (semantischen / pragmatischen) Ebene zu unterscheiden ist.

Digitale Daten sind insofern besondere Güter, als sie unkörperlich (= im physikalischen Sinn immateriell[3]), aber zugleich nur trägergebunden existieren können. Hinzu kommt, dass digitale Daten einer nicht-rivalen, verlustfreien und einer – spätestens nach Veröffentlichung – nicht-exklusiven Nutzung zugänglich sind. Dies unterscheidet digitale Daten als Informationsträger von anderen analogen Informationsträgern, wie etwa einer handgeschriebenen Papiernotiz. Letztere – der analoge Informationsträger - lässt sich nicht verlustfrei reproduzieren und zugleich nur rival sowie exklusiv nutzen, weil die Papiernotiz ein „natürlich knappes" Gut ist. Letztlich ist aber auch die Papiernotiz nur bloßer Informationsträger, wie auch die digitalen Daten, sodass die jeweils repräsentierte Information davon zu unterscheiden ist. **Information** ist für sich genommen stets unkörperlich, nicht notwendig trägergebunden sowie ihrer Natur nach einer nicht-rivalen, nicht-exklusiven Nutzung zugänglich.

Vereinfachtes Beispiel: Der Temperatur-Messwert „38,3" kann durch Zuordnung zum Rind mit der Ohrmarkennummer „AT 99 1701 555" zur Information über dessen Körpertemperatur werden. Diese Information kann in unterschiedlicher Form „transportiert" werden (Analog als Ablesung vom Thermometer und Notiz durch den Veterinär oder in Form digitaler Daten). Binär codiert wäre der Datensatz „38,3; AT 99 1701 555;" folgendermaßen gestaltet: „110011 111000 101100 110110 111011 100000 1000001 1010100 100000 111001 111001 100000 110001 110111 110000 110001 100000 110101 110101 110101 111011 1101 1010 1101 1010" und solcherart elektronisch, optisch oder magnetisch auf einem Datenträger gespeichert.

[1] Art 2 Z 1 DGA VO 2022/868.

[2] ISO/IEC 2382:2015 Information technology — Vocabulary.

[3] Im Unterschied zu körperlichen Objekten, die im physikalischen Sinn als Materie und folglich äußerlich (räumlich) abgegrenzt und solcherart beherrschbar sind. Vgl *Helmich* in *Kletečka/Schauer,* ABGB-ON1.05 § 292 Rz 6; *Holzner in Rummel/Lukas,* ABGB4 § 292 Rz 2.

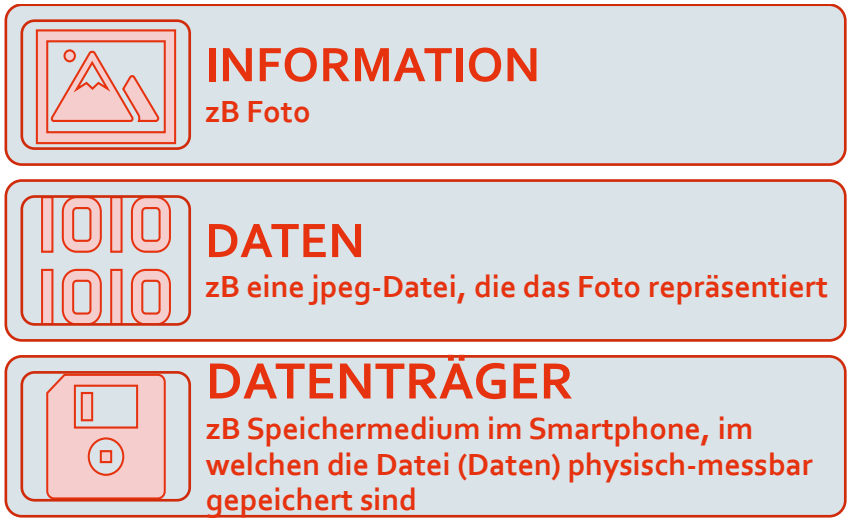

Abbildung 2: Information, Daten und Datenträger

Aus rechtlicher Sicht ergeben sich damit unterschiedliche Anknüpfungsobjekte: a) die digitalen „Daten" als Informationsträger und b) die „Information" an sich. Die folgenden Darstellungen setzen auf dieser Trennung von Daten und Information an, wenngleich im Schrifttum mitunter diese Begriffe synonym gebraucht werden.

Zivilrechtliche Bewertung

Für die zivilrechtliche Beurteilung bildet zunächst § 285 ABGB, der den **Sachbegriff** definiert, den Ausgangspunkt. Diese Bestimmung, die dem unveränderten Bestand des ABGB idF JGS 946/1811 angehört und in ihrer Reichweite dem Institutionensystem[4] des ABGB geschuldet ist, definiert als „Sache" (oder im weiten Verständnis „Rechtsobjekt"[5]) im rechtlichen Sinn *„[a]lles, was von der Person unterschieden ist, und zum Gebrauche der Menschen dient"*. Kennzeichnend für die Qualifikation als Sache im Rechtssinn sind nach herrschender Meinung zwei Merkmale: a) Verschiedenheit von natürlichen Personen und die b) Beherrschbarkeit. In der Lehre wird teils auch auf die Knappheit des Gutes abgestellt,[6] was jedoch iE für die Subsumption als Sache nicht zweckmäßig erscheint.[7]

Fraglich ist im interessierenden Zusammenhang, ob (digitale) Daten und Information dem Sachbegriff unterliegen. Das Kriterium der **Verschiedenheit von der Person** ist im Fall von Daten oder Information unproblematisch erfüllt: Die Abgrenzung wird – soweit ersichtlich – allein in einem körperlichen Sinn vorgenommen, sodass allein ausschlaggebend ist, ob der fragliche Gegenstand integraler Bestandteil des Körpers eines lebenden Menschen ist.[8] Überlegungen dahin, personenbezogene Information als „Teil der Person" zu qualifizieren, bestehen bisweilen nicht. Konsequenz einer solchen Lesart wäre, dass diese als integraler Bestandteil eines Menschen – zumindest Zeit Lebens – nicht als Sache gelten

[4] Nach diesem römisch-rechtlichen Gliederungssystem wird das Privatrecht in zwei große Bereiche, dem „Personenrecht" und dem „Sachenrecht", unterschieden. Kennzeichnend für das Institutionensystem ist der weite Sachbegriff, denn die res umfassen Rechtsobjekte schlechthin, folglich auch unkörperliche Gegenstände und Rechte. Insofern ist § 285 ABGB auch stärker in einem rein programmatischen Sinn zu verstehen (Stabentheiner in Fenyves/Kerschner/Vonkilch, Großkommentar zum ABGB - Klang Kommentar: 353 - 379 ABGB, Sachenrecht. (2011), § 285 Rz 2.), sodass sich daraus zumindest keine unmittelbaren Rechtsfolgen ableiten.

[5] Stabentheiner in Fenyves/Kerschner/Vonkilch, Großkommentar zum ABGB - Klang Kommentar (2011), § 285 ABGB Rz 4.

[6] Eccherer/Riss in Koziol/Bydlinski/Bollenberger, Kurzkommentar zum ABGB: Allgemeines Bürgerliches Gesetzbuch, Ehegesetz, Konsumentenschutzgesetz, IPR-Gesetz, Rom I- und Rom II- und Rom III-VO5 (2017), § 285 ABGB Rz 3.

[7] Stabentheiner in Fenyves/Kerschner/Vonkilch, Großkommentar zum ABGB - Klang Kommentar (2011), § 285 ABGB Rz 11.

[8] S ua Stabentheiner in Fenyves/Kerschner/Vonkilch, Großkommentar zum ABGB - Klang Kommentar (2011), § 285 ABGB Rz 5 ff.

würde und iE rechtsgeschäftlicher Disposition grds entzogen oder zumindest nur eingeschränkt zugänglich wäre. Der herrschenden Ansicht folgend lassen sich Daten und (auch personenbezogene) Information aber als vom Menschen verschieden verstehen, sodass dieses Merkmal erfüllt ist.

Das Kriterium der **Beherrschbarkeit** folgt aus der gesetzlichen Anforderung, dass der Gegenstand dem menschlichen Gebrauch dienlich sein solle. Sache kann zunächst nur etwas sein, das geeignet ist, irgendein menschliches Interesse zu befriedigen. Zur weiteren Konkretisierung hat die Lehre das Kriterium der (faktischen) Beherrschbarkeit entwickelt, wodurch ubiquitäre Güter – wie etwa die freie Luft oder das Wasser im offenen Meer – dem Sachbegriff entzogen sind. Der hier vorgenommenen begrifflichen Trennung von Daten und Information folgend, sind für beide Phänomen unterschiedliche Lösungsansätze zu vertreten: Der ubiquitäre und volatile Charakter von Information, die bereits rein gedanklich und vollkommen trägerlos existieren kann, entzieht diese mangels Beherrschbarkeit selbst dem weiten Sachbegriff des ABGB. Beherrschbar ist allein der jeweilige Informationsträger, mag dieser körperlich (Papiernotiz oder Tonband) oder auch unkörperlich (digitale Daten) sein. Die Information selbst bleibt unbeherrschbar: So lässt sich etwa eine geheime Information zu Papier bringen und dieses Papier in einem Safe „beherrschen". Erlangt aber ein Dritter – in welcher Weise auch immer[9] – von der geheimen Information eines Anderen Kenntnis, zeigt sich, dass die Information selbst nicht beherrschbar ist, zumal der Gedanke im menschlichen Geist des Dritten unstrittig unbeherrschbar und sogar rechtlich geschützt (§ 16 ABGB, Grundrechte) ist. Beherrschbar sind aber digitale Daten, die Informationen repräsentieren. Sie sind zwar unkörperlich, aber physikalisch messbar (außerhalb des menschlichen Geistes) existent, etwa als Lochkarte, magnetischer Zustand oder elektrischer Ladungszustand. Demnach sind Daten – dem hier vertretenen Verständnis folgend – als Sache zu qualifizieren; Information jedoch nicht.

Faktisch kann Information ein knappes Gut und solcherart ein „Vermögenswert" sein, dies liegt aber weniger in der Natur der Information an sich, sondern vielmehr in der Kontrolle der Informationsträger und des Zugangs zu ihr. Der Vermögenswert wird allein durch faktische Zugangskontrolle oder einen sondergesetzlichen[10] Verwertungsschutz begründet. Insofern ist auch kein Grund ersichtlich, aus einem verknappten Informationszugang abzuleiten, Information als Sache im Rechtssinn zu qualifizieren. Ein solche Qualifikation ist uE auch nicht angezeigt, um Transaktionen in der Datenwirtschaft zu beschreiben.

Im Lichte des § 292 ABGB stellt sich weiters die Frage, ob (digitale) Daten als körperliche oder unkörperliche Sache gelten. Bisweilen wurde diese Thematik in Bezug auf Software (Computerprogramme) in der Judikatur behandelt.[11] Dabei ist es vor allem die Besonderheit der Verschränkung physikalisch unkörperlicher (digitaler) Daten mit einem körperlichen Datenträger, ohne den die Daten wesensimmanent nicht existieren können,[12] welche die klare rechtliche Einordnung erschwert. In der Rechtsprechung wurde die dauerhafte Überlassung von Standardsoftware auf Datenträgern gegen Einmalentgelt

[9] ZB eigener Gedanke, Nachforschung (Reverse Engineering) bis hin zum unrechtmäßigen Erlangen des Geheimnisses beim ursprünglichen Geheimnisträger.

[10] Immaterialgüterrechte schützen allesamt nicht die Information als Information, sondern stets nur ihre Verwertung. Die Information

[11] S dazu OGH 2 Ob 625/90, RdW 1991, 230 = wbl 1991, 270 = ecolex 1991, 531; 5 Ob 504/96, SZ 70/202 = JBl 1998, 577 = RdW 1998, 127 = ecolex 1998, 127 (Wilhelm).

[12] Vgl iZm Software: Kisslinger in *Fenyves/Kerschner/Vonkilch*, Großkommentar zum ABGB - Klang Kommentar (2011), § 292 ABGB Rz 15 unter Hinweis auf P. Bydlinski, AcP 198 (1998), 288 (306).

als Kauf einer beweglichen körperlichen Sache qualifiziert.[13] Allerdings anerkennt der deutsche Bundesgerichtshof[14] bereits in einem älteren Urteil zur Softwareüberlassung ohne Übergabe eines Datenträgers, das dem Datenträger nur eine Transportfunktion zukommt und der wirtschaftliche Zweck – namentlich das Nutzbarmachen des Programms – sowohl durch Übergabe der Software auf einem Datenträger, als auch durch bloßes „Überspielen" der Software erreicht wird. Insofern darf – auch mit Blick auf die aktuellen Distributionsformen – die Funktion des körperlichen Datenträgers nicht überbewertet werden. Vielmehr ist die rechtliche Natur der Sache „Software" – oder hier konkret „Daten" – wohlunabhängig vom physischen Substrat zu beurteilen. Damit spricht vieles für die Einordnung als unkörperlich iSd § 292 ABGB.[15]

Sachenrechtliche Fragen stellen sich demnach nur hinsichtlich (digitaler) Daten verstanden als unkörperliche Informationsträger. Information an sich ist indes dem sachenrechtlichen Eigentum wohl bereits mangels Sachqualität entzogen und allein Gegenstand der Querschnittsmaterie „Informationsrecht", wozu insb Immaterialgüterrecht, Wettbewerbsrecht und Datenschutzrecht zählen.

Nach herrschender Ansicht, aber nicht unumstrittener Ansicht sind unkörperliche Sachen – und damit Daten – dem subjektiven **Eigentumsrecht gemäß § 354 ABGB** entzogen. Die hA begründet dies, idR mit Blick auf die deutsche Rechtslage (§ 90 deutsches Bürgerliches Gesetzbuch[16] iZm § 903 deutsches Bürgerliches Gesetzbuch[17]), mit dem Wortlaut des § 354 ABGB. Die Bestimmung des § 354 ABGB statuiert, dass *„[a]ls ein Recht betrachtet, […] Eigenthum das Befugniß [ist], mit der Substanz und den Nutzungen einer Sache nach Willkühr zu schalten, und jeden Andern davon auszuschließen.*" Mangels „*Substanz*", was nach herrschender Ansicht iSe Materialität zu verstehen ist, scheidet eine Anwendung des sachenrechtlichen Eigentums auf unkörperliche Sachen aus.[18]

Zwingend ist diese Sichtweise jedoch nicht, zumal der Sachbegriff des ABGB naturrechtlicher Prägung ist und folglich grds jedwede Form von Vermögensgegenstand als Sache im Rechtssinn subsumiert werden kann. Weiters lässt § 309 iVm § 311 ABGB Besitz an jedweder Sache zu, was § 312 ABGB dahin spezifiziert, dass etwa unkörperliche Sachen „*durch den Gebrauch derselben im eigenen Nahmen*" in Besitz genommen werden können. Und daran schließt § 353 ABGB scheinbar konsequent an: Eigentum ist „*alles, was jemanden zugehöret, alle seine körperlichen und unkörperlichen Sachen*". Dieses weite Eigentumsverständnis spiegelt sich auch in der grundrechtlichen Eigentumsgarantie wider, zumal etwa der Eigentumsbegriff des Art 5 StGG weit verstanden wird und alle vermögenswerten Privatrechte und nach Teilen der Lehre auch vermögenswerten Rechte des öffentlichen Rechts umfasst.[19] Allerdings definiert § 353 ABGB ausdrücklich das Eigentum im „objektiven Sinn", konturiert sohin das gesamte Aktivvermögen einer Person. Die Bestimmung lässt aber Inhalt und Ausmaß der Befugnisse der Eigentümerin bzw. des Eigentümers offen.[20] Insofern ist uE aus den Vorschriften zum Besitz und aus § 353 ABGB wenig zu gewinnen, wenn § 354 ABGB, der das sachenrechtliche Eigentum ausgestaltet, im engen Sinn ausgelegt und auf körperliche Sachen beschränkt verstanden wird. Letztlich wird es aber dem

[13] 5 Ob 504/96, SZ 70/202 = JBl 1998, 577 = RdW 1998, 127 = ecolex 1998, 127 (Wilhelm); 7 Ob 94/02b.

[14] BGH 18.10.1989, VIII ZR 325/88 = NJW 1989, 320.

[15] Kisslinger in *Fenyves/Kerschner/Vonkilch*, Großkommentar zum ABGB - Klang Kommentar (2011), § 292 ABGB Rz 19. S auch Eccherer/Riss in *Koziol/Bydlinski/Bollenberger,* ABGB5 (2017), § 292 ABGB Rz 1.

[16] Die Bestimmung lautet: „§ 90 Begriff der Sache. Sachen im Sinne des Gesetzes sind nur körperliche Gegenstände."

[17] Die Bestimmung lautet: „§ 903 Befugnisse des Eigentümers. Der Eigentümer einer Sache kann, soweit nicht das Gesetz oder Rechte Dritter entgegenstehen, mit der Sache nach Belieben verfahren und andere von jeder Einwirkung ausschließen."

[18] Kiehtaibl in *Fenyves/Kerschner/Vonkilch,* Großkommentar zum ABGB - Klang Kommentar (2011), § 354 ABGB Rz 1. S auch Leupold in *Fenyves/Kerschner/Vonkilch,* Großkommentar zum ABGB - Klang Kommentar (2011), § 353 ABGB Rz 3.

[19] Leupold in *Fenyves/Kerschner/Vonkilch,* Großkommentar zum ABGB - Klang Kommentar (2011), § 353 ABGB Rz 12.

[20] Leupold in *Fenyves/Kerschner/Vonkilch,* Großkommentar zum ABGB - Klang Kommentar (2011), § 353 ABGB Rz 3 und 5.

OGH obliegen zu entscheiden, ob der Substanzbegriff des § 354 ABGB tatsächlich Körperlichkeit voraussetzt.

Daten als Sache nehmen – im Unterschied zu abstrakt-gedanklichem Vermögen, wie Information oder Rechte – eine Sonderstellung ein, weil sie über den Datenträger physikalisch objektivierbar sind und insofern ein – wenn auch physikalisch unkörperliches, aber messbares – Substrat aufweisen, welches sich als Anknüpfungspunkt für das sachenrechtliche Eigentum eignet und eine objektive – nach außen hin erkennbare – Zuordnung theoretisch ermöglicht. Die auf einem USB-Stick gespeicherte Datei ließe sich zwanglos iSd § 354 ABGB einer Person zuordnen, ungeachtet des Eigentums am körperlichen Datenträger (USB-Stick). Es wäre dabei auch schlüssig, dass sachenrechtlich zwischen Datenträger und den darauf gespeicherten Daten differenziert wird. Wenn dem Datenträger wirtschaftlich betrachtet nur Transportfunktion zukommt und die gespeicherten Daten ein selbstständig verkehrsfähiges Gut sind,[21] erscheint es wenig überzeugend, gespeicherte Daten als bloßen Zustand der Substanz des Datenträgers anzusehen. Dies spiegelt auch in keiner Weise eine Lebensrealität wider, in der digitale Güter tagtäglich millionenfach Transaktionsgegenstand sind.

Aber das Bedürfnis nach einer (sachenrechtlichen) Entkoppelung von Datenträger und Daten rechtfertigt nicht zwingend eine Anwendung des Eigentumsrechts iSd § 354 ABGB auf Daten. Vielmehr sprechen gute Gründe gegen ein sachenrechtliches Eigentum an Daten („Dateneigentum"). Das Eigentum iSd §§ 354 ff ABGB ist doch iE stark von der Vorstellung einer Zuweisung körperliche Objekte geprägt. MaW das sachenrechtliche Eigentum ist in seiner Detailausgestaltung klar auf körperliche Objekte zugeschnitten:

Dies beginnt bereits bei der Frage des originären Eigentumserwerbs, denn die Bestimmungen der §§ 381 ff ABGB (Zueignen, Finden, Zuwachs, Verarbeitung) legen ihrer Ausgestaltung nach einen auf körperliche Objekte abstellenden Sachbegriff nahe. Im Schrifttum wird in diesem Kontext mitunter auf den „Skribenten" abgestellt. Demgemäß soll demjenigen das Dateneigentum zukommen, der die Speicherung der Daten unmittelbar selbst bewirkt.[22]

Zudem könnte fraglich sein, wie weit bei Daten das Rechtsobjekt konturiert ist und ob nicht bloß ein konkreter Datensatz, sondern auch alle Kopien desselben von einem einheitlichen Eigentumsrecht erfasst wären. Dagegen spricht der sachenrechtliche Spezialitätsgrundsatz: Sachenrechte können grds nur an bestimmten, genau bezeichneten Sachen – nicht an Sachgesamtheiten – begründet werden. Folglich müssten die Sachenrechte für jede einzelne (klar abgegrenzte) Kopie der Daten gesondert begründet werden, was angesichts der Volatilität digitaler Daten zu nicht unerheblichen Rechtsunsicherheiten führen kann, zumal ein gutgläubiger Eigentumserwerb bei unkörperlichen Sachen jedenfalls ausscheidet (§ 354 ABGB).

Schließlich ist der Schutzumfang des sachenrechtlichen Eigentums und die darauf begründeten Ansprüche stark auf körperliche Gegenstände ausgerichtet: Vereinfacht gesagt, schützt das Eigentumsrecht den Eigentümer vor einer Beeinträchtigung der materiellen Integrität des Eigentumsobjekts und soll eine Rückführung des Gegenstands vom Nichtberechtigten ermöglichen. Im Fall von (digitalen) Daten ist aber neben dem Schutz der Integrität und der Möglichkeit der Herausgabe vom nichtberechtigten Dritten, vor allem der Schutz vor ungerechtfertigter Kopie von zentraler Bedeutung. Letzterer ist aber dem sachenrechtlichen Eigentumsrecht fremd und wird nur etwa durch das Urheberrecht erzielt. Schließlich ist aber auch der Herausgabeanspruch, ein zentraler Anspruch des Eigentümers, im Zusammenhang mit digitalen Daten unscharf, zumal unklar ist, ob eine Herausgabe – die bei digitalen

[21] BGH 18.10.1989, VIII ZR 325/88 = NJW 1989, 320.

[22] S dazu ua *Dürager*, Sind Daten ein schutzfähiges Gut?, ÖBl 2018, 260 (262).

Daten immer auf ein Kopieren und/oder Übermitteln hinausläuft – zugleich auch eine Löschung beim Verpflichteten erfordert.[23] Könnte etwa im Fall urheberrechtlich geschützter Inhalte eine zulässig hergestellte Privatkopie (iSd § 42 UrhG) der das Werk repräsentierenden Daten einer solchen Löschungsverpflichtung entgegengehalten werden, zumal die Kopie als neue Sache mit eigenem rechtlichen Schicksal zu beurteilen wäre?

UE ist eine Ausdehnung des § 354 ABGB dem Wortlaut nach nicht per se ausgeschlossen, aber iE aus teleologischen Erwägungen abzulehnen. Ein gewisse (wohl geringe) Rechtsunsicherheit bleibt bis zur höchstgerichtlichen Klärung wohl bestehen.

Damit ergeben sich folgende zusammenfassenden Schlussfolgerungen:

- **Landwirtschaftliche Information können nicht als Sachen im Rechtssinn qualifiziert werden, weil Information ubiquitärer Natur und für sich genommen nicht beherrschbar ist. Dessen ungeachtet kann diese Information durch Immaterialgüterrechte „verdinglicht" werden oder auch durch Wettbewerbs- sowie Datenschutzrecht geschützt werden.**
- **(Digitale) Daten sind unkörperliche Sachen im Rechtssinn. Sie können Gegenstand des Besitzes, nicht aber des sachenrechtlichen Eigentums iSd § 354 ABGB sein. Demnach kennt das österreichische Zivilrecht kein „Dateneigentum".**
- **Digitale Daten, die landwirtschaftliche Information repräsentieren, können – ungeachtet der sachenrechtlichen Dimension – schuldrechtlicher Transaktionsgegenstand sein. Demgemäß bestimmt allein die faktische Kontrolle über die Daten die Bandbreite an Transaktionsmöglichkeiten, die im Rahmen der Privatautonomie ausgeübt werden können. Dabei bilden die Gesetz- und Sittenwidrigkeit sowie ein allenfalls bestehender Kontrahierungszwang die zivilrechtlichen Grenzen des Handlungsspielraums jener Personen, die faktische Kontrolle über die Daten haben.**

Urheberrechtliche Bewertung

Das Urheberrecht schützt eigentümliche geistige Schöpfungen als Werke auf den Gebieten der Literatur, der Tonkunst, der bildenden Kunst und der Filmkunst.[24] Die Katalog von Werkarten des § 1 UrhG ist abschließend, eröffnet jedoch innerhalb der jeweiligen Kategorien durchaus weite Anwendungsfelder. Aus dem Schutzbereich des Urheberrechts fallen demnach insb technische Erfindungen als solche sowie Duft und Geschmack[25]. Der urheberrechtliche Schutz als Werk setzt neben der Einordnung der zu prüfenden Schöpfung in einer der vorgenannten Kategorien voraus, dass a) eine **geistige Schöpfung** vorliegt und sich darin b) ein gewisses Maß **Originalität oder Individualität** (Eigentümlichkeit) widerspiegelt. Der Werkbegriff des Urheberrechts ist **zweckneutral und objektiv**. Demgemäß wird kein besonderer ästhetischer, künstlerischer oder wissenschaftlicher Wert verlangt. Auch ein reiner Gebrauchszweck schadet nicht.[26]

[23] Vgl BGH 17.04.1996, VIII ZR 5/95, zur – allerdings nicht auf sachenrechtliche Grundlagen gestützten -Herausgabe einer Kundenliste bei gleichzeitiger Löschung beim Verpflichteten.

[24] § 1 Abs 1 UrhG.

[25] EuGH C-310/17.

[26] *Ciresa,* Österreichisches Urheberrecht, § 1 UrhG Rz 3 f.

Eine **geistige Schöpfung** iSd § 1 UrhG liegt vor, wenn einem geistigen Stoff in sinnlich wahrnehmbarer und konkreter Form Ausdruck verliehen wurde. Dabei ist aber nicht gefordert, dass die Schöpfung körperlich fixiert oder tatsächlich von einer anderen Person als dem Schöpfer wahrgenommen wird. Demgemäß entsteht das Werk bereits durch Formung eines gedanklichen Stoffes und seiner Äußerung (zB durch mündlichen Vortrag), gleichgültig ob diese Äußerung von einem Dritten tatsächlich wahrgenommen wird. Es genügt vielmehr die Äußerung – also der formgewordene Gedanke des Schöpfers – an sich. Das Urheberrecht erfasst nur konkrete Ausgestaltungen eines gedanklichen Stoffes, nicht aber die Ideen und gedanklichen Konzepte als solche. Ausgeschlossen sind demnach auch Algorithmen, Motive, mathematischen Lehren, wissenschaftliche Erkenntnisse, historische Fakten, etc. Schöpfungen müssen nach hA Ergebnis eines persönlichen Denkprozesses sein: Dies folgt aus dem Kriterium des geistigen Schaffens, bei dem es sich um eine auf Gestalten gerichtete, genuin menschliche Tätigkeit handelt. Demgemäß kann etwa an maschinengenerierten Schöpfungen auch kein Urheberrecht entstehen, wenn kein Mensch einen zurechenbaren eigenschöpferischen Beitrag zur Schöpfung geleistet hat.

Das Erfordernis der **Eigentümlichkeit** setzt voraus, dass sich in der Schöpfung „die Persönlichkeit des Schöpfers widerspiegelt". Die Schöpfung muss demnach so individuelle Züge aufweisen, dass sie den Stempel der Einmaligkeit und Zugehörigkeit zum Schöpfer trägt.[27] Das UrhG geht von einem werkartübergreifenden Maßstab aus, der nicht allzu hoch angesetzt ist und auch Schöpfungen von geringer Eigentümlichkeit („kleine Münze") schützt. Der Beurteilungsmaßstab ist auch zunehmend durch die Rechtsprechung des EuGH determiniert, wobei dieser an die Originalität keine allzu hohen Anforderungen anlegt. Demnach bleibt nur das Alltägliche, Landläufige, üblicherweise Hervorgebrachte sowie rein handwerkliche, routinemäßige Leistungen urheberrechtlich schutzlos.[28] Individualität setzt Gestaltungsspielraum voraus, sodass Schöpfungen die ausschließlich durch äußere Sachzwänge[29] oder ihre technische Funktion[30] bestimmt sind, mangels Originalität schutzlos bleiben.

Das Urheberrecht entsteht kraft gesetzlicher Anordnung durch den Realakt der Schöpfung unmittelbar in der Person des Schöpfers. Eine Registrierung ist ebenso wenig erforderlich, wie eine Kennzeichnung der Schöpfung mit einem Urhebervermerk.

Das Urheberrecht folgt dem **Schöpferprinzip**. Demnach ist diejenige natürliche Person Urheberin bzw. Urheber, die das Werk geschaffen hat.[31] Die volle Geschäftsfähigkeit der Schöpferin bzw. des Schöpfers ist für das Entstehen des Urheberrechts unbedeutend, weil der Schutz durch Realakt und nicht durch rechtsgeschäftlichen Willen entsteht. Das Urheberrecht schützt das ideelle Band zwischen Schöpferin/Schöpfer und Schöpfung durch das Urheberpersönlichkeitsrecht (§ 19 ff UrhG). Dieses bildet in Gemeinschaft mit den Verwertungsrechten (§§ 14 ff UrhG) das subjektive Urheberrecht in Form eines untrennbaren Bündels an Rechten, das unter Lebenden unübertragbar und nach herrschender Ansicht unverzichtbar ist. Wie das sachenrechtliche Eigentum ist auch das Urheberrecht ein absolutes Recht, das erga omnes wirkt.

---

[27] StRsp, insb OGH 4 Ob 317/78, ÖBl 1978, 107.

[28] OGH 4 Ob 162/08i – Schokoladenschuh, MR 2008, 362 (Walter); OGH 4 Ob 34/93 – Hermes Symbol, ÖBl 1993, 132 = MR 1993 (Walter) = ecolex 1993, 688.

[29] *Appl,* Technische Standardisierung und Geistiges Eigentum, 103 (104 f). OGH 11.06.2018, 4Ob101/18h – *Zeitungsschütten II,* ZTR 2018,179 = MR 2018,280 (Walter) = ecolex 2018/495 S 1106 (Tonninger) - ecolex 2018,1106 (Tonninger) = GRUR Int 2019,600.

[30] *Kucsko in Kucsko/Handig,* urheber.recht2 § 1 UrhG Rz 58; *Rauer in Götting/Lauber-Rönsberg/Rauer,* BeckOK UrhR38 UrhG § 2 Rn. 63.

[31] § 10 Abs 1 UrhG.

Das Urheberrecht schützt im Lichte der einleitenden Ausführungen Schöpfungen – formgewordene Gedanken – in ihrer abstrakten Existenz, ungeachtet des Bestands körperlicher Fixierung. Folglich besteht etwa das Urheberrecht an einem Digitalfoto selbst dann fort, wenn dessen Digitaldaten und Ausdrucke vernichtet sind. Das Urheberrecht schützt digitale Daten – nach eingangs beschriebenem Verständnis – ebenso wenig wie bspw Papier und Druckerschwärze. Digitale Daten oder Papier und Druckerschwärze können Werke repräsentieren, sie sind aber nicht selbst das Werk. Eine Sprachschöpfung (zB ein Roman) kann in Form eines E-Books oder gedruckten Buches erscheinen. Die Schöpfung als Schutzobjekt existiert dabei aber unabhängig vom Werkträger als ubiquitäres geistiges Gut. Damit erklärt sich auch der Umstand, dass mit dem bloßen Eigentum an einem gedruckten Buch – also an Papier und Druckerschwärze – oder aus der faktischen Kontrolle digitaler Daten keinerlei urheberrechtlichen Befugnisse ableiten.[32] Der bloße Besitz digitaler Daten indiziert demnach nicht, dass eine Berechtigung zur Verwertung der darin repräsentierten, geschützten Werke.

Soweit landwirtschaftliche Informationen als Werk iSd UrhG qualifiziert werden können und folglich Urheberrechte daran bestehen, indiziert die bloße faktische Verfügungsmacht über den Werkträger (zB digitale Daten) für sich genommen nicht das Bestehen urheberrechtlicher Verfügungsmacht.

Angesichts des idR „technischen" Charakters der im interessierenden Zusammenhang relevanten landwirtschaftlichen Informationen ist deren urheberrechtliche Schutzfähigkeit mit Blick auf das Kriterium der Eigentümlichkeit fraglich. Gleiches gilt für maschinengenerierte Informationen, an deren Schöpfung kein Mensch eigenschöpferisch beteiligt war. Auch ihnen fehlt die urheberrechtliche Schutzfähigkeit, mangels geistigen Schaffens. Mit Blick auf das Leitszenario wird eine urheberrechtliche Schutzfähigkeit in vielen Bereichen nicht vorliegen, was jedoch im konkreten Einzelfall zu prüfen ist.

Wenngleich für einzelne landwirtschaftliche Informationen, zB die einzelnen durch einen LIDAR-Scan von Weinbaufluren in der Wachau gesammelten Datenpunkte oder die einzelnen Gesundheitsinformation von Nutztieren, keine Urheberrechte bestehen werden, kann sich in ihrer Sammlung eine urheberrechtlich schutzfähige Schöpfung manifestieren: § 6 UrhG stellt etwa auch Sammlungen von Beiträgen zu einem einheitlichen Ganzen unter urheberrechtlichen Schutz, wenn sich in Auswahl und Anordnung der Beiträge eine eigenschöpferische Leistung widerspiegelt. Der Schutz erstreckt sich demgemäß auch nicht auf die einzelnen Beiträge, sondern allein auf den durch die Originalität der Zusammenstellung erzielten „Mehrwert". Schutzbegründend ist demnach nicht die Qualität der Beiträge, sondern der originäre Leitgedanke der Sammlung. Datenbankwerke[33] (§ 40f UrhG) sind ein Unterfall des Sammelwerks. Für sie ist kennzeichnend das die Beiträge, dh die einzelnen Datenbankelemente, systematisch oder methodisch angeordnet und einzeln mit elektronischen Mitteln oder auf andere Weise zugänglich sind. Auch hier muss sich – wie bei den Sammelwerken – in der Datenbankarchitektur die schöpferische Originalität widerspiegeln.

Im gegenständlichen Kontext sind Sachverhalte denkbar, in denen sich in der Zusammenstellung an sich schutzloser landwirtschaftlicher Informationen ein urheberrechtlich geschütztes Sammel- oder Datenbankwerk iSd § 40f UrhG realisiert.

Neben dem urheberrechtlichen Schutz ieS regelt das UrhG auch sogenannte verwandte Schutzrechte (Leistungsschutzrechte). Dazu zählen der Schutz von Darbietungen (§§ 66 ff), der Lichtbildschutz (§§ 73 ff UrhG), das Schallträgerherstellerrecht (§§ 76 ff UrhG) sowie der Schutz von Rundfunksendungen (§ 76a UrhG). Ergänzend zum urheberrechtlichen Schutz für Datenbanken besteht auch ein paralleler sui-generis Schutz, der – wie auch der urheberrechtliche Schutz der Datenbanken – auf die Datenbank-

[32] S dazu § 33 Abs 2 UrhG.

[33] Die Regelungen der § 40f ff UrhG gehen auf die Datenbank-RL zurück.

RL zurückgeht. Gegenstand das **Sui-Generis-Schutzrechts für Datenbankhersteller** sind Datenbanken nur dann, wenn für die Beschaffung, Überprüfung oder Darstellung ihres Inhalts eine nach Art oder Umfang wesentliche Investition erforderlich war.[34] Folglich stellt das Sui-Generis-Schutzrecht nicht auf eine bestimmte Qualität der Datenbankstruktur ab, sondern allein auf die Signifikanz der für die Beschaffung, Überprüfung oder Darstellung des Inhalts erforderlichen Investition. Gefordert ist demnach eine mit Blick auf die Datenbank „wesentliche" Investition, sohin eine gewisse Investitionshöhe. Unbeachtlich sind dabei die unmittelbaren Kosten der Erzeugung von Datenbankelementen. Zu berücksichtigen sind nur Kosten der Datensammlung, -beschaffung, -sichtung, -zusammenstellung und -darstellung. Lassen sich diese Kosten nicht von den Kosten der Erzeugung von Datenbankelementen trennen, sind sie zur Gänze unbeachtlich.[35] Die Kosten müssen nicht quantitativ, sondern auch qualitativ „wesentlich" sein, sodass „Allerweltsinvestitionen" unbeachtlich sind. Datenbankhersteller und originäre/r Inhaberin/Inhaber des Schutzrechts ist die/derjenige, die/der die wesentliche Investition vorgenommen hat. Eine Datenbank setzt wesensimmanent eine innere Ordnung voraus, sodass unstrukturierte „Datenhaufen" definitionsgemäß ausscheiden.

Datenbanken mit landwirtschaftlichen Informationen können dem Sui-Generis-Datenbankrecht iSd § 76c UrhG unterliegen, wenn für die Datensammlung, -sichtung, -auswertung und -darstellung eine nicht bloß unerhebliche Investition getätigten worden ist. Kosten der – idR kostspieligen – Informationsgewinnung bleiben aber unbeachtlich.

Damit ergeben sich folgende zusammenfassenden Schlussfolgerungen:

- **Formgewordene landwirtschaftliche Information ist nur dann urheberrechtlich schutzfähig, wenn sie a) sich unten den abgeschlossenen Kreis schutzfähiger Werkkategorien subsumieren lässt, b) zumindest teilweise das Ergebnis menschlichen Schaffens ist und c) ein Mindestmaß an Originalität aufweist. Dies wird mit Blick auf das Leitszenario (der Erzeugung, Sammlung und Verarbeitung landwirtschaftlicher Daten und Information) jedoch die Ausnahme sein.**
- **Wenngleich im Regelfall die einzelne formgewordene Information für sich genommen schutzlos bleibt, kann ihre Aggregation zu einem urheberrechtlich schutzfähigen Datenbankwerk führen, wenn sich in der Datenbankarchitektur (Auswahl und Anordnung) ein eigenschöpferischer Leitgedanke manifestiert.**
- **Neben dem Datenbankurheberrecht kommt auch dem Sui-Generis-Datenbankschutzrecht (§ 76c UrhG) eine relevante Rolle zu. Schutzvoraussetzung ist das Vorliegen einer wesentlichen Investition in Bezug auf Sammlung, Überprüfung und Darstellung der Datenbankelemente. Die Kosten der Informationsgewinnung sind indes unbeachtlich.**

[34] § 76c UrhG.

[35] EuGH C-203/02; s dazu Wiebe in Spindler/Schuster (Hg), Recht der elektronischen Medien3, § 87a dUrhG Rz 10 ff.

Geschäftsgeheimnisschutz

Die im Leitszenario angeführten landwirtschaftliche Informationen (Landmaschinendaten, Tiersensordaten, landwirtschaftliche Betriebsdaten sowie Daten über Bewirtschaftung und Bodennutzung landwirtschaftlicher Flächen) können allesamt als Geschäftsgeheimnisse geschützt sein. Geschäftsgeheimnisse sind sowohl strafrechtlich (vgl insb §§ 122 f StGB) als auch zivilrechtlich (§§ 26a ff UWG) geschützt, wobei im gegenständlichen Kontext vor allem der zivilrechtliche Schutz von Bedeutung ist. Dem Schutz unterliegt das Geheimnis, sohin die geheime Information an sich, aber ebenso Daten und andere Informationsträger, aus denen sich die geheimen Informationen erschließen lassen.[36]

Voraussetzung des Schutzes als Geschäftsgeheimnis ist gem § 26b Abs 1 UWG, dass eine Information (kumulativ) **geheim**, aufgrund des Geheimnischarakters von **kommerziellem Wert** und Gegenstand **angemessenen Geheimhaltungsmaßnahmen** ist. Diese Definition kann sowohl auf die Landmaschinendaten, Tiersensordaten, landwirtschaftliche Betriebsdaten sowie Daten über Bewirtschaftung und Bodennutzung landwirtschaftlicher Flächen zutreffen.

Entscheidend ist insb, ob diese Informationen den erforderlichen **Geheimnischarakter** aufweisen. Dazu dürfen sie weder in ihrer Gesamtheit noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen zu tun haben, allgemein bekannt noch ohne weiteres zugänglich sein. Allgemein bekannt wären etwa landwirtschaftliche Betriebsdaten, die aus öffentlich einsehbaren Verzeichnissen (zb Firmenbuch, Grundbuch) erschlossen werden können. Dasselbe gilt für Wetterdaten, die aus öffentlich zugänglichen Quellen (zB Internetseiten) ersichtlich sind. Ebenso keinen Geschäftsgeheimnisschutz genießen sämtliche Informationen über einen Landwirtschaftsbetrieb, die durch das Einsehen des Betriebs von der Straße[37] aus erschlossen werden können oder die zum allgemeinen Wissensstand einer durchschnittlichen Fachperson auf dem jeweiligen Gebiet (sohin im Bereich der Landwirtschaft oder der Landmaschinen etc) zählen. Letztendlich fehlt auch all jenen Informationen der Geheimnischarakter, wenn diese einer unbestimmten und unbegrenzten Anzahl von Personen (insb wenn diese nicht durch Vertraulichkeitsverpflichtungen gebunden sind) mitgeteilt werden. Werden etwa in einem Landwirtschaftsbetrieb Führungen für betriebsexterne Personen durchgeführt, sind die Informationen, die dabei ersichtlich werden, nicht (mehr) als Geschäftsgeheimnis geschützt. Der Geheimnischarakter ist insb fraglich, wenn Informationen aus einer Untersuchung der Landmaschinen (Reverse Engineering) erschlossen werden können. Dabei ist strittig, ob diesen Informationen bereits der Geheimnischarakter an sich fehlt, oder ob diese grds als Geschäftsgeheimnis geschützt sind, in der Folge aber gem § 26d Abs 2 Z 2 UWG erschlossen werden dürfen.

Insofern wird zu unterscheiden sein: Kann ein technisch versierter Interessent Informationen durch einfachste Beobachtungen und Untersuchungen (zB durch das Öffnen einer Abdeckung einer Maschine) erschließen, sind diese von vornherein nicht geheim;[38] dagegen sind Informationen, die sich nur durch aufwendige technische Untersuchungen oder chemischer Analysen gewinnen lassen, als Geschäftsgeheimnisse zu qualifizieren, jedoch dürfen diese aus Produkten oder Gegenständen, die öffentlich verfügbar gemacht wurden oder sich im rechtmäßigen Besitz der Erwerberin bzw. des Erwerbers der Information befindet, der keiner rechtsgültigen Pflicht zur Beschränkung des Erwerbs des Geschäftsgeheimnisses unterliegt, erschlossen und in der Folge auch genutzt werden.

[36] Vgl insb § 26c Abs 1 Z 1 UWG

[37] Vgl BGH I ZR 56/07 – *Betriebsbeobachtung,* GRUR 2009, 1075.

[38] Vgl *Schönknecht* in Keller/Schönknecht/Glinke (Hrsg), Geschäftsgeheimnisschutzgesetz (2021) § 3 Rz 28.

Als weitere Voraussetzungen müssen Geschäftsgeheimnisse durch **angemessene Geheimhaltungsmaßnahmen** geschützt werden. Dabei kommen sowohl faktische (Passwortschutz, Zugangsbeschränkungen etc) als auch rechtliche (Geheimhaltungsvereinbarungen) Maßnahmen in Betracht. Ob getroffene Maßnahmen ausreichend sind, ist im jeweiligen Einzelfall (insb auch in Anbetracht der Branche und der Größe des Unternehmens)[39] zu beurteilen. Jedenfalls sind weder bestmögliche noch sicherste Maßnahmen erforderlich, umgekehrt reicht aber auch ein Minimum an Schutz nicht aus.[40] Aufgrund der Relevanz der Unternehmensgröße ist aber davon auszugehen, dass bei kleineren Landwirtinnen bzw. Landwirten bereits geringere Geheimhaltungsmaßnahmen ausreichen, während bei größeren Landwirtschaftsbetrieben strengere Maßnahmen erforderlich sind.

Inhaberschaft: Inhaberin bzw. Inhaber eines Geschäftsgeheimnisses ist diejenige natürliche oder juristische Person, welche die rechtmäßige **Verfügungsgewalt** über das Geschäftsgeheimnis besitzt (§ 26b Abs 2 UWG), sohin den Zugriff auf das Geschäftsgeheimnis bestimmen, einschränken oder ausschließen kann und dazu rechtlich befugt ist.[41] Insofern können für Landmaschinendaten, Tiersensordaten, landwirtschaftliche Betriebsdaten sowie Daten über Bewirtschaftung und Bodennutzung landwirtschaftlicher Flächen – sofern diese als Geschäftsgeheimnisse geschützt sind – jeweils unterschiedlichen Personen als Geschäftsgeheimnisinhaber iSd § 26b Abs 2 UWG zu qualifizieren sein.[42] Zu beachten ist, dass der zivilrechtliche Geschäftsgeheimnisschutz und die Definition des Inhabers iSd § 26b Abs 2 UWG das Geschäftsgeheimnis nicht ausschließlich einer Person „zuordnen", sondern dieser Abwehrrechte gegenüber anderen Personen vermitteln, welche das Geheimnis iSd § 26c UWG unberechtigt erwerben (zB durch Betriebsspionage), nutzen oder offenlegen (zB durch das Einstellen ins Internet oder Ausplaudern).[43]

Mit Blick auf das Leitszenario ergeben sich folgende differenzierten Schlussfolgerungen:

— **Betriebliche Daten, die im Farm-Management-System des Herstellers *FMS* erfasst und verwaltet sowie in dessen zentraler Cloud gespeichert werden**: Werden diese Informationen im Betrieb *LW* hervorgebracht (zB Daten und Dokumentationen über die Bodennutzung, Pflegemaßnahmen und Ertrag, Daten über Art/Menge des verwendeten Düngers oder Daten über die Abnehmer der Erzeugnisse), ist die Inhaberin bzw. der Inhaber des landwirtschaftlichen Betriebs als Geheimnisinhaber iSd § 26b Abs 2 UWG zu qualifizieren. Dabei ist unerheblich, wenn diese im Betrieb erzeugten Informationen durch Dienstnehmerinnen bzw. Dienstnehmer hervorgebracht wurden.[44] Auch schadet es nicht, wenn diese Informationen in dem Farm-Management-System des Herstellers FMS erfasst und/oder auf dessen externer Speicherinfrastruktur (Cloud) gespeichert sind.[45] Fraglich ist, ob im Fall der Speicherung in der externen Cloud *FMS* (neben *LW*) als Geheimnisinhaber zu qualifizieren ist. Mit der Rechtsprechung ist jedenfalls davon auszugehen, dass der Cloudanbieter *FMS* gegen Personen vorgehen kann, die sich unberechtigterweise Zugriff auf den Server der Cloud verschaffen.[46] Dagegen ist der Cloudanbieter aufgrund der vertraglichen Verpflichtung gegenüber *LW* idR aber nicht berechtigt,

[39] ErlRV 375 BlgNR 26. GP 3.

[40] OLG Hamm 4 U 177/19, MMR 2021, 506.

[41] OGH 4 Ob 182/20y - *Ärztesoftware* - Produktfamilie *S.*

[42] Siehe zum Problem insb *Leistner/Antoine/Sagstetter,* Big Data 156 ff.

[43] *Hofmarcher,* Das Geschäftsgeheimnis Rz 2.63.

[44] *Hofmarcher,* Das Geschäftsgeheimnis Rz 2.71; *Ohly* in Ohly/Sosnitza, Gesetz gegen den unlauteren Wettbewerb8 GeschGehG § 2 Rz 25.

[45] Vgl *Alexander* in Köhler/Bornkamm/Feddersen, UWG41 GeschGehG § 2 Rz 98: sonstige Kontrollmöglichkeiten technischer Art sind ausreichend (zB die Kontrolle der Zugriffsrechte auf Daten, die auf einem Server gespeichert sind).

[46] OGH 4 Ob 165/16t – *Ticketsysteme.*

dessen Geschäftsgeheimnisse offenzulegen oder selbst zu nutzen. Der *FMS* ist insofern grds nur zur Abwehr, nicht aber zur einer selbstständigen Wahrnehmung von Verwertungsmöglichkeiten berechtigt. Letzteres erfordert vertragliche Regelungen.-

- **Daten zur Planung betrieblicher Vorgänge aus externen Datenquellen (zB Wetterdaten)**: Sofern diese Informationen als Geschäftsgeheimnisse zu qualifizieren sind, ist originäre/r Inhaberin/Inhaber des Geheimnisses iSd § 26b Abs 2 UWG nicht *LW*, sondern derjenige, der diese externen Informationen hervorgebracht hat (zB der Inhaber des Unternehmens, in dem die Wetterdaten gemessen wurden). *LW* kann in der Folge aber derivativ (aufgrund eines Kauf- oder Lizenzvertrags) an dem Geschäftsgeheimnis berechtigt sein.[47] Auch die nicht ausschließliche Berechtigung an den Informationen wäre erfasst.[48] In diesem Fall wären dann grds sowohl der externe Hersteller als auch LW berechtigt, Verletzungen des Geschäftsgeheimnisses durch Dritte geltend zu machen.[49]
- **Daten des Nutzviehs (smarte Ohrmarken)**: Die durch Ohrmarken des Nutzviehs erzeugten Informationen (zB Standort und Gesundheitsdaten) entstehen im Betrieb von LW durch Tiere, die in dessen Eigentum stehen. Insofern ist LW als Unternehmensinhaber grds auch bzgl dieser Informationen Geschäftsgeheimnisinhaber iSd § 26b Abs 2 UWG. Dass diese Informationen *LW* nur beschränkt und innerhalb der proprietären Softwareumgebungen der Herstellerin bzw. des Herstellers zugänglich sind, ändert daran grds nichts: Dass die Speicherung auf einer der Herstellerin bzw. dem Hersteller gehörenden Speicherinfrastruktur erfolgt, ist unerheblich.[50] Relevant ist aber der Umstand, dass *LW* lediglich beschränkten Zugang zu diesen Daten genießt und diese lediglich über die proprietäre Softwareumgebung der Herstellerin bzw. des Herstellers nutzen kann. Insofern ist seine Verfügungsgewalt iSd § 26b Abs 2 UWG faktisch (proprietäre Umgebung) und ggf rechtlich (Nutzungsbedingungen) eingeschränkt. Die Konsequenzen für den Geschäftsgeheimnisschutz sowie die Rechte und Pflichten im Verhältnis *LW* zur/zum Herstellerin/Hersteller bedarf dann einer eingehenden Analyse des zwischen diesen bestehenden Vertrags. Soweit die Verfügungsgewalt von *LW* reicht, ist dieser aber grds zur Geltendmachung von Ansprüchen gegenüber Dritten befugt, welche diese geheimen Information iSd § 26c UWG unrechtmäßig erwerben, nutzen oder offenlegen. Ebenso wird die Herstellerin bzw. der Hersteller gegen Dritte vorgehen können, die sich unberechtigterweise Zugriff auf diese Information verschaffen.[51]
- **Daten der smarten Landmaschinen des Herstellers *LMH***: Werden diese geheimen Informationen (zB Nutzungs- und Sensordaten) durch den Gebrauch von Maschinen generiert, die im **Eigentum des *LW*** stehen, und sind diese Daten auf Speichermedien gespeichert, auf die ausschließlich der *LW* Zugriff hat, ist grds dieser als Geschäftsgeheimnisinhaber iSd § 26b Abs 2 UWG zu qualifizieren. Dass diese Informationen ggf auf einer externen Speicherinfrastruktur des *LMH* gespeichert sind und ggf auch von diesen eingesehen werden können, ändert nichts daran, dass der *LW* Ansprüche auf Basis von §§ 2a ff UWG geltend machen kann, wenn Dritte diese Daten unberechtigterweise erschließen, nutzen oder offenlegen.[52] Wenn die erzeugten

[47] OGH 4 Ob 182/20y - *Ärztesoftware - Produktfamilie S.*

[48] OGH 4 Ob 182/20y - *Ärztesoftware - Produktfamilie S.*

[49] Siehe dazu näher *Hofmarcher,* Das Geschäftsgeheimnis Rz 2.67.

[50] Siehe dazu oben bei den betrieblichen Daten, die im Farm-Management-System des Herstellers FMS erfasst und verwaltet sowie in dessen zentraler Cloud gespeichert werden.

[51] Siehe dazu oben bei den betrieblichen Daten, die im Farm-Management-System des Herstellers FMS erfasst und verwaltet sowie in dessen zentraler Cloud gespeichert werden.

[52] Ob dem *LMH* in diesem Fall ebenso zum Mitinhaber des Geschäftsgeheimnisses wird, ist fraglich; in der Lit wird dies bejaht (vgl *Leistner/Antoine/Sagstetter,* Big Data 157). Jedenfalls wird der *LMH* Abwehransprüche geltend machen können, wenn sich Dritte unberechtigt Zugriff auf den Server verschaffen (vgl OGH 4 Ob 165/16t – *Ticketsysteme)*.

Daten jedoch ausschließlich dem *LMH* zugänglich und kann der *LW* diese Daten nicht erschließen (zB wenn Landmaschinen Daten live auf einen Server der Herstellerin bzw. des Herstellers abspeichern und der *LW* auf diese Daten keinen Zugriff hat), ist (ausschließlich) der *LMH* als Inhaber dieser Geschäftsgeheimnisse zu qualifizieren. Werden diese Daten durch Hinzuziehung von **Landmaschinen-Dienstleister** generiert, die ihrerseits smarte Landmaschinen einsetzen und Daten erzeugen sowie sammeln, ist entscheidend, wer auf die Daten Zugriff hat und welche Regelungen im Rechtsverhältnis zwischen dem LW und dem Dienstleister getroffen wurden.[53] Haben ausschließlich die Dienstleister Zugriff auf die generierten Daten, werden es grds diese sein, die die Verfügungsmacht über die im Zuge des Einsatzes gesammelten Daten haben und daher als Geschäftsgeheimnisinhaber iSd § 26b Abs 2 UWG zu qualifizieren sind. In der Literatur wird allerdings vertreten, dass wenn vertrauliche Information außerhalb der eigenen Unternehmenssphäre – aber im Auftrag des Unternehmensinhabers – entstehen (zB im Rahmen eines Werkvertrags), die Inhaberschaft unter Berücksichtigung der zwischen den Parteien getroffenen Abrede zu ermitteln ist.[54] Freilich wird der zwischen dem *LW* und dem Landmaschinen-Dienstleister bestehende Vertrag idR die Erbringung von landwirtschaftlichen Dienstleistungen und nicht die Generierung von Daten zum Inhalt haben; dennoch ist nicht auszuschließen, dass aufgrund des Vertragsverhältnisses (auch) der *LW* zum Inhaber des Geschäftsgeheimnisses iSd § 26b Abs 2 UWG werden kann. Ähnliche Grundsätze gelten, wenn Landmaschinen von einem **Landmaschinen-Verleiher** *LMV* angemietet werden. Werden Landmaschinen **gemeinschaftlich von mehreren Betrieben genutzt**, ist zunächst zu ermitteln, wer die faktische Zugriffsmöglichkeit auf die erzeugten Daten hat.[55] Haben mehrere LW Zugriff auf die generierten Daten, können diese gemeinsam Inhaber der Geschäftsgeheimnisse iSd § 26b Abs 2 UWG sein.

— **Betriebsdaten unterschiedlicher landwirtschaftlicher Betriebe von *FMS***: Geheime Informationen, die der Farm-Management-System Herstellers über verschiedene landwirtschaftliche Betriebe sammelt, sind grds als dessen Geschäftsgeheimnisse zu qualifizieren, da er über diese Informationen die Verfügungsgewalt iSd § 26b Abs 2 UWG hat. Dass diese Informationen Auskünfte über die Landwirtinnen und Landwirte erschließen und im datenschutzrechtlichen Sinn ggf einen Personenbezug aufweisen, ändert nichts daran, dass es sich bei ihnen um Geschäftsgeheimnisse des FMS handeln kann, wodurch diesem die Abwehransprüche der §§ 26a ff UWG zustehen.

Reichweite des Schutzes: Hinsichtlich der Reichweite verleiht der zivilrechtliche Geheimnisschutz dem Inhaber keine ausschließliche Befugnis, über ein Geschäftsgeheimnis zu verfügen. MaW wird das Geschäftsgeheimnis dem Geheimnisinhaber nicht absolut zugeordnet, was insb darin ersichtlich ist, dass die unabhängige Entdeckung oder Schöpfung eines Geschäftsgeheimnisses (auch durch einen Konkurrenten) zulässig ist (vgl § 26d Abs 2 Z 1 UWG) und die Nutzung in der Folge keinen Beschränkungen unterworfen ist. Der Geschäftsgeheimnisschutz verleiht dem Geheimnisinhaber damit nur zivilrechtliche Ansprüche (insb auf Unterlassung, Beseitigung und Schadenersatz)[56] gegen Personen, welchen den Geheimnischarakter unberechtigt überwinden (zB durch Betriebsspionage) und dadurch einen Tatbe-

[53] Vgl zur Relevanz privatautonomer Vereinbarungen *Leistner/Antoine/Sagstetter,* Big Data 157.

[54] *Alexander* in Köhler/Bornkamm/Feddersen, UWG41 GeschGehG § 2 Rz 101; Ohly in Ohly/Sosnitza, Gesetz gegen den unlauteren Wettbewerb8 GeschGehG § 2 Rz 25.

[55] *Hofmarcher,* Das Geschäftsgeheimnis Rz 2.64.

[56] §§ 26e ff UWG.

stand des unrechtmäßigen Erwerbs iSd § 26d UWG erfüllen. Ebenso erfasst wäre Fälle der unrechtmäßigen Nutzung oder Offenlegung eines Geschäftsgeheimnisses iSd § 26d UWG (zB wenn Dienstnehmerinnen bzw. Dienstnehmer nach dem Ausscheiden unrechtmäßig erlangte Geschäftsgeheimnisse des *LW* als ehemaligen Dienstnehmers verwerten).

Implikationen aus den EU Digital Rechtsakten (DSGVO, DGA, Data Act)

Datenschutz-Grundverordnung (DSGVO)

Neben den bereits erwähnten Rechtsmechanismen trägt auch das Datenschutzrecht zur Kontrolle von Informationen bei. Aber auch das Datenschutzrecht vermittelt kein Daten- oder Informationseigentum – sind aber die Anwendungsvoraussetzungen erfüllt, wird durch Schutzrechte dem Betroffenen eine Einflussnahme auf die Verarbeitung ermöglicht.

Anders als im Zivil- oder Urheberrecht oder im Geschäftsgeheimnisschutz gilt das europäische Datenschutzrecht (DSGVO) nicht für alle Formen von Informationen. Art 2 DSGVO schränkt die Anwendung der Rechtsvorschriften auf *personenbezogene* Daten – dh im eingangs beschriebenen Sinn „Informationen" – ein. Das sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Personen) beziehen. Darunter sind sowohl persönliche Informationen, wie den Namen oder die Anschrift, als auch Kommunikationsdaten und erkennbare Bildaufnahmen zu verstehen.[57]

Gerade im landwirtschaftlichen Umfeld werden viele Informationen in Form digitaler Daten gesammelt, die dieser Qualifikation auf den ersten Blick nicht entsprechen. So sind Informationen über Wetterverhältnisse, Wachstumsraten oder Nutztiere grds ohne Bezug auf eine natürliche Person. Ein Personenbezug kann aber auch entstehen, wenn etwa eine Drohne bei der Feldüberwachung Aufnahmen der Kinder des Nachbar-LW erstellt oder eine Agrar-Maschine bei Inbetriebnahme nach der Benutzerkennung des Mitarbeiters fragt. Es kommt nämlich nicht auf das Verarbeitungsziel, sondern auf die tatsächlich verarbeiteten Informationen an, solange diese später auch wahrnehmbar sind – etwa in der Videoaufzeichnung.[58] Die natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung entscheidet, ist gem Art 4 DSGVO „Verantwortlicher".

Da somit die DSGVO auch im „Smart-Farming" unstrittig eine wichtige Rolle spielt, sind die Schutzrechte der betroffenen Personen näher zu beleuchten. Besonders relevant ist das Recht auf Berichtigung, das Recht auf Einschränkung der Verarbeitung und das Recht auf Löschung der personenbezogenen Informationen. Gem Art 16 DSGVO hat ein Betroffener das Recht von einem Verantwortlichen die Änderung von Informationen zu fordern, wenn diese falsch oder unvollständig sind. Die betroffene Person muss auch kein besonderes Interesse an der Änderung geltend machen. [59] Falsche oder unvollständige Informationen stellen grds immer eine Gefahr für den Betroffenen dar.[60]

Parallel zu diesem Änderungsanspruch kann gem Art 17 DSGVO auch ein Löschungsanspruch bestehen. Vereinfacht gesagt hat ein Betroffener immer dann einen Anspruch seine personenbezogenen Informationen löschen zu lassen, wenn die Verarbeitung unrechtmäßig erfolgt. Besonders relevant kann dies etwa sein, wenn ein LW der Verarbeitung seiner personenbezogenen Informationen durch einen

[57] *Hödl* in Knyrim (Hsg), DatKomm (2018) Art 4 DSGVO Rz 9.
[58] *Herbst in Kühling/Buchner* (Hsg), DS-GVO Art 4 Nr 2 Rz 21
[59] *Worms* in Wolff/Brink/v. Ungern-Sternberg (Hg), BeckOK DatenschutzR 44 (2021), DS-GVO Art. 16 Rn. 46
[60] *Haidinger* in Knyrim (Hsg), DatKomm (2018) Art 17 DSGVO Rz 1.

Anbieter von LW-Software zustimmt – die Zustimmung aber nicht den Anforderungen der DSGVO entspricht oder im Nachhinein widerrufen wird.

Anders als das Änderungsrecht wird das Löschungsrecht aber durch bestimmte Ausnahmebestimmungen eingeschränkt. Hat die/der Verantwortliche etwa gesetzliche Pflichten die Informationen aufzubewahren oder werden sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, kann der Betroffene sein Recht nicht mehr voll durchsetzen. Diese Interessenabwägung zeigt bereits, dass die DSGVO nicht darauf abzielt, den Betroffenen die volle Informationsherrschaft zu verschaffen, sondern ihn lediglich vor Gefahren der Informationsverarbeitung schützen will. Daher kommt es auch regelmäßig zur Interessensabwägung zwischen Betroffenem und Verarbeiter.

Auch das Recht auf Einschränkung der Verarbeitung dient im Kern der Abwägung der Interessen der beteiligten Personen.[61] Bestreitet etwa ein LW die Richtigkeit seiner personenbezogenen Informationen oder erhebt er Einspruch gegen die Verarbeitung, kann er vom Verantwortlichen verlangen, die Verarbeitung seiner personenbezogenen Informationen für die Dauer der Überprüfung der Angaben auszusetzen. In dieser Zeit kann der Verantwortliche die betroffenen Informationen des LW nur speichern oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen verwenden. Darüber hinaus ist eine Verarbeitung dann rechtmäßig, wenn der Verantwortliche die Rechte einer anderen Person schützt oder ein wichtiges Interesse der Union oder eines Mitgliedstaates besteht.

Zusammenfassend ist festzuhalten, dass die Rechte der/des Betroffenen durchaus Ähnlichkeiten zu absoluten Verfügungsrechten eines Eigentümers aufweisen. In beiden Fällen besteht ein absolutes Recht mit erga omnes Wirkung, Dritten gegenüber kann daher ein gewisses Verhalten oder Unterlassen rechtlich abverlangt werden. Die Rechte des Datenschutzes richten sich aber primär darauf, mögliche Gefahren vom Betroffenen durch eine rechtswidrige Datenverarbeitung abzuwenden. Das Eigentumsrecht geht darüber aber hinaus und erlaubt, unabhängig von einer möglichen Beeinträchtigung geschützter Interessen, über die eigenen Sachen iSv Vermögensgegenständen frei zu verfügen (zB die Sache zu verkaufen oder zu verschenken). Weiters weisen die Betroffenenrechte in der DSGVO auch oftmals Ausnahmen oder bestimmte Anwendungsvoraussetzungen auf, die ihre Wirksamkeit in der Praxis beschränken.

Die DSGVO bietet daher keine Alternative zu absoluten Rechten über das Eigentum, sondern gewährt eine beschränkte Datenhoheit in bestimmten Gefahrensituationen.

Data Governance Act

Neben der DSGVO ist bereits eine weitere EU-Verordnung seit Juni 2022 in Kraft, die der Regulierung von Informationen dient. Der Data Governance Act (DGA) soll insb die Nutzung von Informationen öffentlicher Einrichtungen erleichtern um damit einen Mehrwert für Wirtschaft, Forschung und andere Bereiche zu schaffen. Gem Art 3 DGA regelt die Verordnung die Weitergabe von „Daten, die sich im Besitz öffentlicher Stellen befinden“.

Zur Definition des „Besitzers der Daten“ bzw. „der Besitzerin von Daten“ nimmt die Verordnung nicht Stellung. Nach dem Regelungszweck ist es naheliegend, damit alle öffentlichen Stellen einzuschließen, die faktische Kontrolle über die Informationen ausüben können und diese den Wirtschaftsteilnehmerinnen und Wirtschaftsteilnehmer damit verheimlichen können. Eine besondere rechtliche Qualifikation, wie etwa der Besitz iSd § 309 ABGB, wird wohl nicht verlangt sein.

[61] *Worms* in Wolff/Brink/v. Ungern-Sternberg (Hg), BeckOK DatenschutzR 44 (2021), DS-GVO Art. 18 Rn. 2

Der DGA verwendet zwar den Begriff des „Besitzes an Informationen", verknüpft mit diesem aber keine rechtliche Qualität, sondern bloß die faktische Herrschaft. Somit führt auch der DGA zu keiner rechtlichen Allokation von Informationen.

Data Act

Eine sektorspezifische Beschränkung wie im DGA kennt der Entwurf des Data Act (DA-E)[62] nicht. Er gilt dabei für personen- wie für nicht-personenbezogene Daten gleichermaßen Die künftige Verordnung soll nicht nur durch neue Zugangs- und Nutzungsrechte den Austausch von Informationen fördern, sondern soll auch einheitliche Standards für den Informationsaustausch zwischen Marktteilnehmer schaffen.[63] Der DA wird auf „vernetzte Produkte" und damit „verbundene Dienste" anwendbar sein.

Während auf die vorgesehenen Zugangsrechte und deren Voraussetzungen im nächsten Abschnitt detailliert eingegangen wird, stellt sich zunächst die Frage ob mit dem DA auch eine rechtliche Zuordnung von Informationen oder Daten erfolgen soll.

Sowohl die DSGVO als auch der DGA nehmen nicht ausdrücklich zu Begriffen wie „Besitzer von Daten" Stellung. Der DA-E nennt dagegen in seinen Begriffsbestimmungen den sogenannten „Dateninhaber". Dieser wird aber nicht als Inhaber über bestimmte Rechte an Informationen definiert, sondern ist lediglich eine Person die *„auf Daten aus dem vernetzten Produkt zugegriffen oder bei der Erbringung eines verbundenen Dienstes Daten erzeugt hat und die das vertraglich vereinbarte Recht hat, diese Daten zu nutzen*".

Die Definition ist somit stark auf die Regelungsziele des DA bezogen und soll nicht zur Einführung eines europäisch determinierten „Dateneigentums" oder „Datenbesitzes" führen.[64] Abseits von einem dinglichen Recht, soll aber auch der DA mehr Kontrolle über Daten schaffen. So ist es der Dateninhaberin bzw. dem Dateninhaber gem Art 4 Abs 6 DA-E nur aufgrund einer vertraglichen Vereinbarung gestattet, Information (Daten) zu verarbeiten auf die er faktisch Zugriff hat. Die Nutzungsgenehmigung darf im Anwendungsbereich des DA-E auch nicht Voraussetzung für den Abschluss eines Vertrags sein, solange die Informationsnutzung nicht für die Vertragserfüllung notwendig ist.

Eine ähnliche Notwendigkeitspflicht findet sich bereits im Rechtfertigungstatbestand der Vertragserfüllung in Art 6 Abs 1 lit b DSGVO – dort jedoch nur mit Wirkung für personenbezogene Informationen.

Zusammenfassend ist daher festzuhalten, dass auch der DA – nach aktuellem Entwurf – keine dinglich wirkende Allokation von Daten oder Information statuiert. Demgemäß bleibt die oben skizzierte zivilrechtliche Beurteilung im Hinblick auf sachenrechtliche Überlegungen unverändert: der DA wird kein „Daten- oder Informationseigentum" im sachenrechtlichen Sinn einführen.

Zugangsrechte zu Daten und Information

Vor dem Hintergrund der faktischen und rechtlichen Allokation von landwirtschaftlichen Daten und Informationen behandelt dieser Abschnitt die Frage, ob und wenn ja, für welche Personengruppen und Zwecke gesetzliche Zugangsrechte bestehen. Ausgangspunkt bildet eine Analyse des allgemeinen Zivilrechts, des Wettbewerbsrechts bis hin zum Urheberrecht.

[62] Data Act-Entw COM/2022/68 final idF EP P9_TA(2023)0069 vom 14.3.2023.
[63] *Heinzke,* Data Act: Auf dem Weg zur europäischen Datenwirtschaft, BB 2023, 201.
[64] ErwG 5 Data Act Entwurf vom 14.3.2023.

Zugangsrechte de lege lata

Zivilrechtliche Ansprüche

Im interessierenden Zusammenhang ergeben sich aus dem allgemeinen Zivilrecht keine Ansprüche dahin, dass derjenige der – insb über den Besitz von Daten – den Zugang zu landwirtschaftlicher Information faktisch kontrolliert, Dritten einen Informationszugang bereitstellen muss. Über digitale Daten, die landwirtschaftliche Informationen repräsentieren, kann im Rahmen der Privatautonomie bis zur Grenze der Gesetz- und Sittenwidrigkeit schuldrechtlich verfügt werden. Ein Kontrahierungszwang besteht im allgemeinen Zivilrecht nicht; dieser kann aber etwa durch das Wettbewerbsrecht oder andere Regulatorien indiziert sein. Insofern bestehen keine zivilrechtlichen Mittel, die Dritten einen Anspruch auf Zugang gegenüber demjenigen gewähren, der den Zugang kontrolliert.

Ggf kann eine rechtsgrundlose Nutzung von digitalen Daten **bereicherungsrechtliche Ansprüche** begründen. Dies führt jedoch nur zu einer Abgeltung erfolgter Nutzungen, verschafft aber nicht zwingend Zugang zu den durch digitale Daten repräsentierten Informationen.

Das allgemeine Zivilrecht vermittelt keine Ansprüche auf Zugang zu digitalen Daten und der solcherart repräsentierten landwirtschaftlichen Information.

Wettbewerbliche Ansprüche

Sowohl das österreichische (§ 4 ff KartG 2005) als auch das europäische Wettbewerbsrecht (Art 102 AEUV) enthalten ein absolutes **Verbot des Missbrauchs einer marktbeherrschenden Stellung**. Für Zwecke dieser Ausführungen wird auf die EU-Rechtslage fokussiert, deren Ergebnisse angesichts vergleichbarer Regelungstatbestände sinngemäß auf das österreichische Recht übertragen werden können.

Schutzgegenstand des Marktmachtmissbrauchsverbots ist in erster Linie der Wettbewerb als Institution, wobei darüber hinaus auch individuelle sowie überindividuelle Interessen der Marktteilnehmer geschützt werden. Die ungerechtfertigte Zugangsverweigerung – etwa in Form der Lizenzverweigerung oder der Verweigerung von Schnittstelleninformation – ist dabei eine typische Erscheinungsform des Marktmachtmissbrauchs.

Adressat des Wettbewerbsrechts sind **Unternehmen**. Ein Unternehmen iSd Art 101 und 102 AEUV ist nach der Judikatur des EuGH *„jede, eine wirtschaftliche Tätigkeit ausübende Einheit, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung*“.[65] Das Wettbewerbsrecht folgt einem funktionalen Verständnis, sodass weniger formale, institutionelle oder organisatorische Kriterien ausschlaggebend sind, sondern im Wesentlichen die wirtschaftliche (marktgerichtete) Natur der Tätigkeit bedeutend ist. Dies liegt idR vor, wenn eine Tätigkeit – zumindest hypothetisch – von einem privaten Unternehmen gegen Entgelt erbracht werden kann. Demgemäß können etwa auch öffentliche Stellen – außerhalb der Wahrnehmung hoheitlicher Verwaltung – im Rahmen der Privatwirtschaftsverwaltung dem Wettbewerbsrecht unterliegen.

Marktmachtmissbrauch setzt zunächst **Marktmacht** voraus. Um diese zu ermitteln, muss zunächst der räumlich, sachlich und zeitlich relevante Markt bestimmt werden. Im interessierenden Zusammenhang liegt der Fokus auf die Frage der sachlichen Marktabgrenzung: Grds umfasst der sachlich relevante Markt *„sämtliche Erzeugnisse und/oder Dienstleistungen, die vom Verbraucher hinsichtlich ihrer Eigen-*

[65] StRsp, EuGH Rs C-41/90 – Höfner u Elser/Macrotron, Slg 1991, I-1979.

schaften, Preise und ihres vorgesehenen Verwendungszwecks als austauschbar oder substituierbar angesehen werden.“[66] Im Fall informationeller Güter, wie im Leitszenario angenommen, ist zu fragen, welche landwirtschaftliche Informationen aus Perspektive der Marktgegenseite substituierbar ist. Die Tatsache, dass eine bestimmte Information nur aus einer bestimmten Quelle bezogen werden kann, führt daher nicht zwangsläufig zu einem Monopol, wenn die fragliche Information tatsächlich durch andere Informationen anderer Anbieter substituierbar ist.
Anders als § 4 KartG 2005 enthält Art 102 AEUV keine Definition der Marktbeherrschung. In der europäischen Spruchpraxis ist Marktbeherrschung eine wirtschaftliche Marktposition eines Unternehmens, “*die dieses in die Lage versetzt, die Aufrechterhaltung eines wirksamen Wettbewerbs auf dem relevanten Markt zu verhindern, indem sie ihm die Möglichkeit verschafft, sich seinen Wettbewerbern, seinen Abnehmern und schließlich den Verbrauchern gegenüber in einem nennenswerten Umfang unabhängig zu verhalten. Das Vorliegen einer beherrschenden Stellung ergibt sich im Allgemeinen aus dem Zusammentreffen mehrerer Faktoren, die jeweils für sich genommen nicht ausschlaggebend sein müssen.*“[67]

Im interessierenden Zusammenhang wird daher im jeweiligen Einzelfall zu prüfen sein, ob am Markt für landwirtschaftliche Information Unternehmen mit Marktmacht beteiligt sind. Dies könnte – je nach Marktstruktur – etwa in Bezug auf Anbieterinnen/Anbieter von Farm Management System, Cloud-Dienstleister, Landmaschinenhersteller oder Landmaschinen-Verleiher zutreffen. Wenngleich auch landwirtschaftliche Betriebe als Unternehmen iSd des Wettbewerbsrechts anzusehen sind, wird ihnen idR am Markt für landwirtschaftliche Daten und Informationen keine Marktmacht zukommen.

Art 102 AEUV pönalisiert jedoch nicht bereits das Erlangen von Marktmacht als solcher, sondern erst ihren Missbrauch. Im interessierenden Zusammenhang sind unterschiedliche Szenarien denkbar.

Die typischen Gattungen des Marktmachtmissbrauchs sind der Behinderungsmissbrauch, der Ausbeutungsmissbrauch und der Marktstrukturmissbrauch. Ein Missbrauch kann – im Unterschied zum Kartellverbot nach § 101 AEUV – grds nicht gerechtfertigt werden; Ausnahmetatbestände oder „Freistellungen“ sind nicht möglich. Grds sind aber legitime Beweggründe im Rahmen einer Interessenabwägung durchaus zu berücksichtigen.

Im interessierenden Zusammenhang sind grds alle Missbrauchsformen denkbar: Zum einen könnten marktmächtige Landmaschinenhersteller, Farm Management System Anbieter oder andere Akteure den Zugang zu ihren Daten und Informationen in unsachlicher Weise verweigern oder Konditionen verlangen, die unter normalen Wettbewerbsbedingungen nicht geltend gemacht werden könnten. Dabei ist vor allem der sog „Hebelmissbrauch“ problematisch, wenn durch Zugangsverweigerung die Marktmacht am Primärmarkt (bspw für smarte Landmaschinen) auf einen nachgelagerten Markt (zB Märkte datengestützte Dienste) ausgedehnt werden soll. Lässt sich ein Marktmachtmissbrauch feststellen, bestehen neben öffentlich-rechtlichen Sanktionen vor allem auch zivilrechtliche Mechanismen, die Marktteilnehmern einen Zugang zu landwirtschaftlicher Information eröffnen könnten.

[66] Bekanntmachung der EK über die Definition des relevanten Marktes im Sinne des Wettbewerbsrechts der Gemeinschaft, ABl 1997 C 372/5.

[67] S insb EuGH Rs 27/76 – United Brands/EK, Slg 1978, 207.

Die Rechtsprechung der Unionsgerichte in den Rechtssachen Magill[68], IMS Health[69], Microsoft[70] und Huawei[71] legen schließlich klar nahe, dass unter bestimmten Voraussetzungen ein Kontrahierungszwang aus dem Wettbewerbsrecht folgt. Im Wesentlichen sind vier Kriterien – ausgehend von der Marktmacht des Unternehmens – maßgeblich, um gestützt auf das Wettbewerbsrecht die Erteilung einer Lizenz zur Nutzung bzw zur Zugangsgewährung einzuklagen: 1) Die Daten sind für das nachgelagerte Produkt unerlässlich, 2) es besteht kein wirksamer Wettbewerb zwischen dem vorgelagerten und dem nachgelagerten Produkt, 3) die Verweigerung verhindert die Entstehung eines nachgelagerten Produkts, und 4) es gibt keinen objektiven Grund für die Verweigerung.[72]

Liegt tatsächlich ein Marktmachmissbrauch etwa durch Verweigerung des Zugangs zu landwirtschaftlichen Informationen vor und lassen sich die Daten als „Essential Facility" verstehen, können Marktteilnehmer Zugang zu FRAND-Konditionen – also zu fairen, verhältnismäßigen und nichtdiskriminierenden Bedingungen – geltend machen. Dieses Instrument ist, wie die Praxis zu standardessentiellen Patenten zeigt, durchaus wirksam, wirft aber regelmäßig auch relevante Probleme in der Praxis auf – insb hinsichtlich der Bemessung fairer Preise und auf Ebene der Durchsetzung.

Im vorliegenden Zusammenhang bedeutet dies, dass das Wettbewerbsrecht – allerdings erst ab einer gewissen (hohen) Schwelle (Marktmacht + Missbrauch) – Zugang zu landwirtschaftlicher zu fairen, verhältnismäßigen und nichtdiskriminierenden Bedingungen eröffnen kann. Insofern sind marktmächtige Marktteilnehmer angehalten, ihre Praxis in Bezug auf den Zugang zu landwirtschaftlicher Information entlang wettbewerbsrechtlicher Rahmenbedingungen auszurichten, was ggf zu einer Öffnung des Zugangs führen kann. Wenn aber proprietäre Informationsquellen brach liegen, also vom Zugangsberechtigten geheim gehalten und nicht benutzt werden, wird auch das Wettbewerbsrecht an seine Grenze stoßen und den Unternehmer nicht zu einer Verwertung zwingen können.

Sonstige Ansprüche, insb im Urheberrecht (Text- und Data Mining)

Sind landwirtschaftliche Informationen Gegenstand urheberrechtlich geschützter Werke, sieht das UrhG diverse Nutzungen vor, die gesetzlich zulässig und vom Urheber daher hinzunehmen sind. Diesen Nutzungen steht das an diesen Werken bestehende Urheberrecht damit nicht im Weg. Zu diesen gesetzlich zulässigen Nutzungen, die im Bereich der Datenwirtschaft relevant sind, zählt insb die Zulässigkeit der Anfertigung flüchtiger und begleitender Vervielfältigungen iSd § 41a UrhG sowie des Text-und-Data-Minings iSd § 42h UrhG.

§ 41a UrhG: Nach dieser Bestimmung ist es zulässig, von urheberrechtlich geschützten Werken vorübergehende Vervielfältigungen anzufertigen, wenn diese (Z 1) flüchtig oder begleitend sind und (Z 2) sie einen integralen und wesentlichen Teil eines technischen Verfahrens bilden und (Z 3) ihr alleiniger Zweck die Übertragung in einem Netz zwischen Dritten durch einen Vermittler oder eine rechtmäßige Nutzung ist (Z 3) sowie ihnen keine eigenständige wirtschaftliche Bedeutung zukommt (Z 4). Exemplarisch erfasst dies etwa Vervielfältigungen in Form von Zwischenspeicherungen, die beim Online-Abruf (iSd Browsings oder Streamings) von Werken in Zwischenspeichern (zB RAM oder Cache Speicher) von

[68] EuGH vbRs C-241/92 P und C-242/91 P – RTE & ITP/EK (‚Magill'), Slg 1995, I-743.

[69] EuGH Rs C-418/01 – IMS-Health/NDC-Health, Slg 2004, I-5038.

[70] EuG Rs T-201/04 – Microsoft/EK, Slg 2007, II-3601.

[71] EuGH Rs C-170/13 – Huawei.

[72] *OV,* COMMISSION STAFF WORKING DOCUMENT on the free flow of data and emerging issues of the European data economy, COM(2017) 9 final 21 f. .

Endgeräten entstehen.[73] Nach dieser Bestimmung ist es etwa zulässig, im Internet (rechtmäßig)[74] bereitgestellte Daten im Wege des Browsings aufzurufen und einzusehen. Vervielfältigungen, die im Zuge von permanenten Downloads ("Herunterladen“) der Werke entstehen, privilegiert diese Bestimmung allerdings nicht.

§ 42h UrhG: Von wichtiger Bedeutung für die Datenwirtschaft ist zudem § 42h UrhG, der Vervielfältigungen von urheberrechtlich geschützten Werken für das sogenannte Text-und-Data-Mining (TDM) gestattet. Dies ist relevant, da sämtliche Vervielfältigungen von urheberrechtlich geschützten Texten oder Daten (zB durch das Einscannen oder Downloaden etc) dem Vervielfältigungsrecht (§ 15 UrhG) des Urhebers unterliegen und grds seiner Zustimmung bedürfen. Aufgrund von § 42h UrhG ist es aber gesetzlich zulässig (und damit nicht von der Zustimmung des Urhebers abhängig), urheberrechtlich geschützte Texte oder Daten zu vervielfältigen (zB abzufotografieren, einzuscannen, herunterzuladen etc), um diese automatisiert auszuwerten und Informationen unter anderem über Muster, Trends und Korrelationen zu gewinnen. MaW gestattet die Bestimmung die Vervielfältigung der Texte und Daten, um die darin enthaltenen Informationen zu erschließen. Allerdings müssen dabei mehrere Voraussetzungen eingehalten werden.

Zweck: Zum einen ist das TDM gem § 42h Abs 1 UrhG für Forschungseinrichtungen (gem Abs 3 leg cit) oder für eine Einrichtung des Kulturerbes (gem § 42 Abs 7 UrhG) zulässig. Der Bereich der Forschung ist iE aber weitgehend auf nichtkommerzielle Forschungsaktivitäten eingeschränkt, da privilegierte Forschungseinrichtungen iSd § 42h Abs 3 UrhG solche sein müssen, die nicht gewinnorientiert sind, alle Gewinne in ihre wissenschaftliche oder künstlerische Forschung reinvestieren oder zwar gewinnorientiert sind und im Rahmen eines staatlich anerkannten Auftrags im öffentlichen Interesse tätig sind. Kommerzielle Forschungszwecke oder generell TDM durch landwirtschaftliche Unternehmen sind daher nicht nach § 42h Abs 1 UrhG zulässig, können aber unter das zulässige TDM zu kommerziellen Zwecken iSd § 42h Abs 6 UrhG fallen.

Rechtmäßiger Zugang: Sowohl das TDM zu Forschungszwecken (§ 42h Abs 1 UrhG) als auch das TDM zu kommerziellen Zwecken (§ 42h Abs 6 UrhG) erfordern einen rechtmäßigen Zugang zu den Daten. Zu Daten besteht ein rechtmäßiger Zugang, wenn dieser von den Rechteinhabern zugelassen (zB aufgrund eines Verkaufs oder einer Vermietung von Daten oder einer Lizenz) oder nicht durch Gesetze beschränkt ist (vgl ErwG 33 InfoSoc-RL). Damit dürfen etwa Daten zu TDM verwendet werden, die auf gekauften, gemieteten oder geschenkten Datenträgern gespeichert sind, im Rahmen von Abo-Zugängen online abrufbar sind oder im Wege des Open-Access im Internet bereitgestellt werden.[75] Unklar ist, ob ein rechtmäßiger Zugang auch zu Daten besteht, die im Internet ohne Zustimmung der Urheber bereitgestellt werden. Rechtssicher lassen sich solche Daten jedenfalls nicht für ein TDM iSd § 42h UrhG verwenden.

Vorbehalte: Das gesetzlich zulässige TDM zu Forschungszwecken kann vertraglich nicht abbedungen werden (§ 42h Abs 5 UrhG). Damit sind Einschränkungen in Nutzungsbedingungen oder Lizenzverträgen, die das TDM zu Forschungszwecken verbieten, unbeachtlich. Anders ist dies jedoch für ein kommerzielles TDM, etwa im Rahmen von landwirtschaftlichen Betrieben. Dazu sieht § 42h Abs 6 UrhG vor, dass das TDM unzulässig ist, wenn „*die Vervielfältigung ausdrücklich verboten und dieses Verbot in angemessener Weise durch einen Nutzungsvorbehalt, und zwar etwa bei über das Internet öffentlich zugänglich gemachten Werken mit maschinenlesbaren Mitteln, kenntlich gemacht*“ wurde. Bei einem

[73] Vgl EuGH 16.7.2009, C-5/08, *Infopaq International/Danske Dagblades Forening.*
[74] Str, vgl aber EuGH 26.4.2017, C-527/15, *Stichting Brein/Wullems [Filmspeler].*
[75] *Homar* in Thiele/Burgstaller, UrhG4 § 42h Rz 56.

solchen (maschinenlesbaren) Vorbehalt dürfen Daten daher nicht für ein kommerziellen Zwecken dienendes TDM verwendet werden und es ist eine Lizenz erforderlich.

Keine „Zugangsrechte“: Sowohl die gesetzlich zulässigen flüchtigen und begleitenden Vervielfältigungen iSd § 41a UrhG, als auch das TDM iSd § 42h UrhG vermitteln aber keine Rechte auf den Zugang zu Daten und Information. Schließlich verlangen beide Bestimmungen eine rechtmäßige Nutzung (§ 41a Z 3 UrhG) oder einen rechtmäßigen Zugang (§ 42h Abs 1 und 6 UrhG). Damit setzt das geltende Urheberrecht voraus, dass die Daten (grds mit Zustimmung der Rechteinhaber) zugänglich sind. Dagegen vermitteln die ggst Bestimmungen aber kein einklagbares Recht darauf, dass Urheber geschützte Daten (ggf in maschinenlesbarem Format) veröffentlichen oder den landwirtschaftlichen Betrieben, die diese gerne nutzen möchten, zugänglich machen.[76]

Kopierschutzmechanismen: Nutzenden ist nicht gestattet – um in den Genuss der zulässigen Nutzungen iSd § 41a UrhG oder § 42h UrhG zu kommen – wirksame technische Maßnahmen iSd § 90c Abs 1 UrhG („Kopierschutzmechanismen“) eigenmächtig beseitigen. Wenn jedoch ein rechtmäßiger Zugang zu Daten besteht, haben Nutzende – die ein TDM iSd § 42h UrhG durchführen möchten – ein einklagbares Rech darauf, dass Rechteinhaber etwaige das TDM verhindernde Kopierschutzmechanismen beseitigen (§ 90c Abs 6 Z 3 UrhG).

Zugangsrechte de lege ferenda

EU Digital Package (Data Act, etc)

Bereits im vorangegangenen Abschnitt wurde der Entwurf des Data Act (DA-E) als neue Regelung für die Datenwirtschaft behandelt, die neue Zugangsrechte zu Informationen vermitteln soll. Diese Rechte können weitrechende Folgen für die verpflichteten Personenkreise haben. Aus diesem Grund wird in diesem Teil der DA näher behandelt, um einen Überblick über die neuen Regelungen der Datenwirtschaft zu bekommen.

Der DA ist weder auf einen bestimmten Typ von Informationen beschränkt (wie etwa die DSGVO) noch trifft er ausschließlich einen bestimmten Sektor (wie der Data Governance Act). Dennoch kennt auch der Verordnungsentwurf bestimmte Grenzen des Anwendungsbereichs.

Anwendungsbereich

Gem Art 1 Abs 2 DA-E sind dessen Regeln nur auf Informationen anzuwenden, die bei der Nutzung von „vernetzten Produkten“ und damit „verbundenen Diensten“ entstehen. „Vernetzte Produkte“ werden vom DA-E als ein physischer Gegenstand definiert, der über seine Nutzung oder Umgebung zugängliche Informationen erlangt und diese weiter übermitteln kann. Gerade im Bereich des Smart Farming ist dies von Relevanz. So werden regelmäßig Sensoren zur Vieh-, Wetter- oder Bodenkontrolle als auch vernetzte LW-Maschinen in den Anwendungsbereich dieser Norm fallen.

Die Definition schließt solche Produkte aus, die Informationen lediglich lokal abspeichern können und über keine Übermittlungsfunktion verfügen. Damit sind wohl etwa Agrar-Drohnen mit einem rein lokalen Speicher für die aufgenommenen Lichtbilder nicht als vernetztes Produkt anzusehen. Weiters werden auch solche Gegenstände ausgeschlossen, deren Hauptfunktion die Speicherung, Verarbeitung und Übertragung von Informationen im Namen Dritter ist. Damit sind Server- oder auch Cloud-Infrastrukturen von der DA-E nicht betroffen.

Neben den „vernetzten Produkten“ werden vom DA-E auch Informationen miteinbezogen, die bei der Verwendung von „verbundene Diensten“ entstehen. „Verbundene Dienste“ sind solche, ohne die ein

[76] *Vgl Homar* in Thiele/Burgstaller, UrhG4 § 42h Rz 70.

„vernetztes Produkt“ seine Funktionen nicht ausführen kann. Die Begriffsbestimmung in Art 2 Abs 2 DA-E als auch die ErwG sprechen dabei von „einer oder mehreren der Funktionen“. Aufgrund dieser weiten Formulierung liegt es nahe, dass ein Dienst nicht ausschließlich für die Hauptfunktion – sondern auch für eine Nebenfunktion eines Produkts notwendig sein kann, um als „verbundener Dienst“ verstanden zu werden

„Verbundene Dienste“ können etwa Steuerungsprogramme für eine selbstfahrende LW-Maschine oder die Betriebssoftware für Bodensensoren sein. Die Informationen, die von diesen Diensten erhoben werden – wie Wartungsintervalle oder Abnützung der Kontaktstellen der Sensoren – sind unabhängig von der Datenerhebung des vernetzten Produkts selbst und können für den Nutzer des Produkts einen eigenen Wert haben.

Betroffene Personen

Ist der Anwendungsbereich des DA-E eröffnet, treffen die darin enthaltenen Rechte und Pflichten vor allem die drei folgenden Personen:

- Nutzerinnen und Nutzer
- Dateninhaberinnen und Dateninhaber
- Datenempfängerinnen und Datenempfänger

Nutzerinnen bzw. Nutzer ist jede Person, die ein „vernetztes Produkt“ besitzt oder einen „verbundenen Dienst“ in Anspruch nimmt. Aus ErwG 18 geht dabei hervor, dass „Besitzer“ derjenige ist, der das Produkt gekauft hat. Aber auch Personen, die auf Grundlage eines Miet- oder Leasingvertrages eine vorübergehende Nutzungsgenehmigung für das Produkt oder den Dienst erhalten, gelten als Nutzerinnen bzw. Nutzer.

Als Dateninhaberin bzw. Dateninhaber wird die Person bezeichnet, die auf die Informationen aus dem vernetzten Produkt oder der verbundenen Leistung Zugriff hat. Wie im vorhergehenden Teil bereits erläutert, führt dieser Begriff nicht zu einer rechtlichen Zuordnung von Informationen zu einer Person iSe „Information- oder Datenbesitzes“. Die Dateninhaberin bzw. der Dateninhaber ist vielmehr die Person, die faktisch Zugriff auf Informationen hat, die durch eine Nutzerin bzw. einen Nutzer bei der Verwendung eines vernetzten Produkts oder einer verbundenen Leistung entstehen.

Im landwirtschaftlichen Bereich werden regelmäßig die Herstellerinnen bzw. Hersteller neuer „Smart-Farming“ Maschinen und die Anbieterinnen bzw. Anbieter von den dafür benötigten Softwarelösungen als „Dateninhaberin bzw. Dateninhaber“ zu qualifizieren sein.

Zuletzt kennt der DA-E auch die Person des Datenempfängers. Dies ist jede Person, der Informationen aus der Nutzung von vernetzten Produkten oder verbundenen Diensten von der Dateninhaberin bzw. vom Dateninhaber auf Verlangen der Nutzerin bzw. des Nutzers oder aufgrund einer rechtlichen Verpflichtung zur Verfügung gestellt werden.

Problematisch ist im Zusammenhang mit diesen Definitionen, dass auf die Überschneidungen nicht eingegangen wird. So wird regelmäßig eine Vermietern bzw. ein Vermieter von LW-Maschinen gegenüber seiner Kundinnen bzw. Kunden die Position einer/eines Dateninhaberin/Dateninhabers aufweisen. Sie/Er selbst kauft die Maschinen aber von der Herstellerin bzw. vom Hersteller und steht diesem wiederum als Nutzerin bzw. Nutzer gegenüber.[77]

[77] *Wolf,* Data Act: "Fair Trade" mit Daten?, ZVR 2023, 232.

Eine weitere Rechtsunsicherheit ergibt sich durch die strikte Anknüpfung der Position einer Nutzerin bzw. eines Nutzers an die Rechtsbeziehung zum „verbundenen Produkt". Gerade in kooperativen LW-Betrieben ist es denkbar, dass aus Kostengründen eine neue „Smart-Farming" Maschine gemeinschaftlich angeschafft wird und dann von den LW des Betriebs ohne Mietvereinbarung, sondern als Betriebsmittel genutzt werden. Folgt man hier dem Wortlaut des Entwurfs, würden wohl die Rechte der Nutzerin bzw. des Nutzers lediglich dem Betrieb zustehen und nicht den einzelnen LW, die die Maschine verwenden.[78]

Zugangsrechte

Grundziel des DA-E ist die Schaffung von mehr Fairness im Datenmarkt und die Zugänglichkeit zu werthaltigen Daten zu erleichtern. Die geplante Verordnung will den Vorteil der faktischen Kontrolle des Dateninhabers über Informationen durch verschiedene Rechte und Pflichten ausgleichen.

Access by Design

Gem Art 3 DA-E sind Herstellerinnen und Hersteller zukünftig dazu verpflichtet, vernetzte Produkte und verbundene Dienste so zu gestalten, dass Nutzerinnen und Nutzer kostenlos, einfach und sicher auf die erhobenen Informationen unmittelbar zugreifen können. Soweit technisch machbar sollen die Informationen in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format verfügbar sein.

Um die Position der Nutzerin bzw. des Nutzers noch weiter zu stärken, muss dieser vor Erwerb des vernetzten Produkts oder verbundenen Dienstes über die Details der Informationserhebung informiert werden. Darüber hinaus muss die Nutzerin bzw. der Nutzer auch über die Art und Weise des kostenlosen Zugriffs auf die Informationen aufgeklärt werden.

Die detaillierten Anforderungen an diese Informationspflicht sind zu begrüßen. Damit wird sichergestellt, dass auch ein Laie eine tatsächliche Möglichkeit erhält seine Rechte in Anspruch zu nehmen. Problematisch ist hier dafür die Frage, wen konkret die Aufklärungspflichten treffen sollen. Im Fall eines Neukaufs einer LW-Maschine von der Herstellerin bzw. vom Hersteller lässt sich diese Frage noch recht leicht beantworten. Werden allerdings vernetzte Produkte zwischen einzelnen LW verkauft, ist wohl unwahrscheinlich, dass die Verkäuferseite den hohen Anforderungen des Verordnungsentwurfs gerecht werden kann.[79]

Ein weiterer Kritikpunkt ist der Umfang des Informationszugangs. So muss die Dateninhaberin bzw. der Dateninhaber auf solche Informationen keinen Zugang gewähren, die durch komplexe proprietäre Algorithmen aus den ursprünglichen Informationen abgeleitet werden. Gerade solche Folgedaten können für die Nutzerin bzw. den Nutzer aber von besonderem Wert sein. Verwendet etwa eine Landwirtin bzw. ein Landwirt Wetter-, Boden- und Vieh- von der selben Herstellerin bzw. vom selben Hersteller können die gemeinsam ausgewerteten Informationen dieser drei Quellen für die weitere Planung der Bodenbestellung entscheidend sein.

[78] Digitalisierung in der Landwirtschaft: Datenschutzrechtliche Herausforderungen, 138.

[79] *Wolf,* Data Act: "Fair Trade" mit Daten?, ZVR 2023, 233.

Access by Request

Sollte es nicht möglich sein, den Nutzerinnen bzw. Nutzern einen unmittelbaren Zugang zu den Informationen – die durch vernetzte Produkte und verbundene Dienste erhoben wurden – zu gewähren, hat die Dateninhaberin bzw. der Dateninhaber gem Art 4 DA-E die Pflicht die Information auf Anfrage der Nutzerin bzw. des Nutzers zur Verfügung zu stellen. Die Informationen sollen dabei grds in der gleichen Form wie unter Abs 3 bereitgestellt werden.

Das Informationsverlangen kann von den Dateninhaberinnen/Dateninhabern abgelehnt werden, wenn der Zugang gegen Unionsrecht oder nationales Recht verstößt. Dies wird regelmäßig der Fall sein, wenn etwa durch ein vernetztes Produkt sensible personenbezogene Daten von Dritten erhoben werden und eine Offenlegung nicht die besonderen Verarbeitungserfordernisse gem Art 9 DSGVO erfüllt. Während mit dieser Situation im medizinischen Umfeld zu rechnen ist, wird es im Bereich der LW wohl eher die Ausnahme bilden.

Art 4 Abs 3 DG-E erlaubt ebenfalls die Einschränkung der Offenlegung aufgrund von Geschäftsgeheimnissen. Kommt es durch die Zugangsgewährung zu den Informationen zur Weitergabe von Geschäftsgeheimnissen der Dateninhaberin bzw. des Dateninhabers, so können vorab „alle Maßnahmen getroffen werden, um die Vertraulichkeit der Geschäftsgeheimnisse gegenüber Dritten zu schützen."

Beruft sich eine Dateninhaberin bzw. ein Dateninhaber auf diese Klausel, muss dies jedenfalls von der Nutzerin bzw. vom Nutzer hinterfragt werden. Grds soll nämlich nur der Zugang zu den erhobenen Informationen der vernetzten Produkte und verbundenen Diensten gewährt werden. Hier ist aber nicht nachvollziehbar, wie es sich dabei um Geschäftsgeheimnisse der Dateninhaberin bzw. des Dateninhabers handeln soll. Die Informationen sind schließlich aus der Verwendung durch die Nutzerin bzw. den Nutzer entstanden.

Access by Third Parties

Gem Art 5 DA-E kann die Nutzerin bzw. der Nutzer von der Dateninhaberin bzw. vom Dateninhaber verlangen, dass diese/dieser die erhobenen Daten an eine dritte Person – den Datenempfänger – weiterleitet. Diese Regelung hat gerade im Bereich der Wartungsdienstleistungen von LW-Maschinen großes Potential. So sollen in Zukunft etwa Werkstätten auf Informationen zugreifen können, die aktuell oftmals nur den Dateninhaberinnen/Dateninhabern – in den meisten Fällen den Herstellerinnen bzw. Herstellern der Maschinen – zugänglich sind.[80]

Art 5 DA-E ergänzt somit den Anspruch auf Datenportabilität gem Art 20 DSGVO nun um nicht-personenbezogene Informationen. Anders als die Regelung in der DSGVO verlangt die Informationsweitergabe von Dateninhaberinnen/Dateninhaber an Datenempfängerinnen/Datenempfänger gem Art 8 DA-E eine vertragliche Vereinbarung zwischen diesen beiden Parteien. Handelt es sich bei Nutzerinnen/Nutzer und Dateninhaberinnen/Dateninhaber um Unternehmerinnen/Unternehmer, kann zweiterer gem Art 9 DA-E auch eine monetäre Gegenleistung für die Informationsbereitstellung verlangen. Diese muss aber diskriminierungsfrei und angemessen sein.

Da LW ihre Agrarmaschinen wohl regelmäßig nicht als Konsumentin bzw. Konsument anschaffen, ist es daher notwendig, beim Kauf von vernetzten Produkten auch die Konditionen für die Informationsbereitstellung auf ihre Rechtmäßigkeit zu prüfen.

[80] *Holm-Hadulla/ Bug/ Pollmeier,* Der Kommissionsentwurf des Data Acts - Ein Überblick, DSB 2022, 108.

Umfang einer rechtlich zulässigen Verwertung

Einer Verwertung von Daten und Information können unter gewissen Umständen Immaterialgüterrechte oder der Schutz von Geschäftsgeheimnissen entgegenstehen. Dort wo diese Schutzsysteme nicht oder nur beschränkt greifen, kommt der Ausgestaltung vertraglicher Beziehungen eine zentrale Rolle zu. In der Folge sollen Möglichkeiten und Grenzen vertragliche Verwertungsbeschränkungen sowie bestehende gesetzliche Beschränkungen dargestellt werden, wie sie für Fälle von Daten- oder Informationstransaktionen typischerweise relevant sind.

Vertragliche Beschränkungen und ihre Grenzen

Wenngleich sich Daten und Information dem Eigentumsbegriff und Information als solche bereits dem zivilrechtlichen Sachbegriff entziehen, sind schuldrechtliche Beziehungen über die Übertragung von Daten oder dem Zugang zu Information unstrittig möglich. Es handelt sich dabei um keine typisierten Verträge des ABGB, sondern um sogenannte Innominatverträge. Diese sind völlig neue Vertragsformen, die allenfalls teilweise von gesetzlichen Vertragstypen erfasst sind, oder um Mischformen bestehender gesetzliche Vertragstypen.[81] Es gilt im österreichischen Recht die Vertragsfreiheit, diese umfasst insb die Inhalts- und Typenfreiheit sowie die Abschlussfreiheit. Ersteres ermöglicht es Verträge jenseits der Vertragstypen des ABGB und mit – weitgehend – beliebigem Inhalt abzuschließen. Die Abschlussfreiheit ist demgegenüber die Freiheit zu entscheiden, ob und mit wem Verträge abgeschlossen werden.[82] Demgemäß besteht bis zur Grenze der Gesetz- und Sittenwidrigkeit gem § 879 ABGB[83] und allenfalls bestehender Kontrahierungszwänge ein großer Spielraum zur Ausgestaltung von Verträgen betreffend Daten oder Information. Dies bedeutet zunächst, dass derjenige, der Daten oder den Zugang kontrolliert, weitreichende vertragliche Gestaltungsmöglichkeiten hat und zudem bis zur Eingriffsschwelle des Wettbewerbsrechts idR keinem Abschlusszwang unterliegt.

In einer von der Europäischen Kommission beauftragten Studie[84] wurde festgehalten, dass in komplexen Datenverträgen die Themen „data ownership“ und Zugang zu Daten adressiert werden. Die entsprechenden Klauseln regeln unter anderem:

- die Möglichkeit einer Partei, Daten weiterzuverwenden oder an Dritte weiterzugeben,
- das „Eigentum“ an den erzeugten/verarbeiteten Daten,
- die Zuweisung etwaiger Rechte an geistigem Eigentum, die durch technische Vorrichtungen erzeugt werden und/oder
- die Frage, inwieweit Parteien, die Zugang zu Daten haben, diese vermarkten dürfen.

Es wurde in der Studie zudem betont, dass eine Vertragspartei regelmäßig versucht, die Verwendung der Daten Zwecke außerhalb der unmittelbaren Vertragserfüllung zu verhindern. Die andere Vertragsseite allerdings selten – mitunter mangels Verhandlungsmacht – hinsichtlich einer weiteren Benutzung der Daten nachverhandelt.[85]

Die zentrale Herausforderung ist demnach die Sicherung fairer Verträge, was dem allgemeinen Zivilrecht im Zusammenhang mit Verträgen über Daten oder Information selbst mit Blick auf das Konsumentenschutzrecht nicht hinlänglich gelingt. Im interessierenden Zusammenhang, namentlich in

[81] *Wiebe in Kletečka/Schauer,* ABGB-ON1.04 § 859 Rz 32.
[82] S zur Vertragsfreiheit, *Grabenwarter/Frank*, B-VG Art 6 StGG Rz 10.
[83] S zu § 879 ABGB: *Krejci in Rummel/Lukas,* ABGB4 § 879 Rz 16ff.
[84] *European Commission/Osborne Clarke LLP.,* Legal study on ownership and access to data: final report. (2016), 79.
[85] COMMISSION STAFF WORKING DOCUMENT on the free flow of data and emerging issues of the European data economy, COM(2017) 9 final, 16.

Rechtsbeziehungen von Landwirtinnen und Landwirten mit anderen Unternehmerinnen und Unternehmern, entfallen konsumentenschutzrechtliche Schutzprinzipien. Insofern sind die Vertragsparteien im B2B-Kontext auf allgemeine zivilrechtliche Vorgaben, allenfalls komplementär ergänzt durch das Wettbewerbsrecht und den neuen Data Act, begrenzt.

Vertragliche Verwertungs- und/oder Benützungsverbote sind idR zulässig und können privatautonom vereinbart werden. Typischer Anwendungsfall wäre etwa im Zusammenhang mit Geschäftsgeheimnissen der sog „Knowhowtransfervertrag", der typischerweise genaue Regelungen hinsichtlich der Benutzung und Verwertung einer als Geschäftsgeheimnis eingestuften Information hat. Aber auch jenseits von geschützter geheimer Information können für nicht geheime Informationen derlei Beschränkungen wirksam vereinbart werden. Dies könnten bspw Daten sein, die bei einer Landwirtin bzw. einem Landwirt entstehen (zB Nutzungsdaten einer Landmaschine), die aber für sich genommen kein Geschäftsgeheimnis – weder des Landwirts noch des Landmaschinenherstellers – darstellen. Über solche Daten kann wirksam verfügt werden und wirksam Verwertungs- oder Verwendungsbeschränkungen vereinbart werden.

Das Problem, das sich bei solchen Daten- oder Informationstransaktionen regelmäßig ergibt, ist die asymmetrische Informationsverteilung in Verbindung mit der unterschiedlichen Verhandlungsmacht zwischen den Parteien. Während große Unternehmen der Datenwirtschaft häufig über die Ressourcen und das Know-how verfügen, um ihre Interessen in Verträgen durchzusetzen, können Landwirtinnen bzw. Landwirte in B2B-Beziehungen oft in eine unterlegene Position geraten.

Dieses Ungleichgewicht, das oftmals auf mangelnde Kenntnis des ökonomischen Werts von Daten oder Information sowie der rechtlichen Rahmenbedingungen seitens der Landwirtinnen bzw. Landwirte zurückgeht, kann dazu führen, dass Landwirtinnen bzw. Landwirte Verträge eingehen, die für sie nachteilig sind, insb wenn diese Daten und Informationen für den individuellen landwirtschaftlichen Betrieb und aber auch überbetrieblich oder für die österreichische Landwirtschaft schlechthin relevant sind. Hier können restriktive Vereinbarungen wichtige Sekundärnutzungen – etwa in der Forschung oder für die politische Entscheidungsfindung – erschweren oder verunmöglichen.

Es wird aber ganz grds zu berücksichtigen sein, dass Information grds „frei" ist und Verwertungs- und Verwendungsbeschränkungen „freier Information" insofern einen nicht unerheblichen Eingriff in die unternehmerische Freiheit darstellen. Dies gilt umso mehr, wenn es sich um (nicht geschäftsgeheimnisgeschützte) Daten oder Informationen handelt, die ihren Ursprung beim vertraglich Beschränkten haben. Die Situation wäre durchaus vergleichbar mit vertraglichen Wettbewerbsverboten, die nur in engen Grenzen (und idR zeitlich befristet) zulässig sind[86].

Gesetzliche Beschränkungen

Der urheberrechtliche Schutz steht der Datennutzung entgegen, soweit Daten oder Informationen urheberrechtlich geschützt sind und die Nutzung nicht unter eine gesetzliche Ausnahme (iSd §§ 41 ff UrhG) fällt oder durch eine vertragliche Erlaubnis („Lizenz") gedeckt ist.

Der Schutz als Geschäftsgeheimnis steht einer Informationsnutzung entgegen, soweit Daten dem Geschäftsgheimnisbegriff iSd § 26b UWG unterfallen und die Nutzung als rechtswidriger Erwerb oder rechtswidrige Nutzung oder Offenlegung iSd § 26c UWG zu qualifizieren ist. Damit steht der Geschäftsgeheimnisschutz der Nutzung der Informationen nicht per se im Weg. Werden diese auf eine Art und

[86] *Graf in Kletečka/Schauer,* ABGB-ON1.05 § 879 Rz 102; *Krejci in Rummel/Lukas*, ABGB4 § 879 Rz 80.

Weise (insb durch eigenständige Erarbeitung oder Reverse Engineering) erworben, ist die weitere Nutzung zulässig. Unzulässig ist jedoch die Nutzung von Geschäftsgeheimnissen, die rechtswidrig (insb durch Betriebsspionage oder durch einen Geheimnisverrat) erlangt worden sind.

Auch durch den Datenschutz wird eine Nutzung von Informationen regelmäßig eingeschränkt. Art 6 DSGVO verlangt für jede Verarbeitung von personenbezogenen Daten einen Rechtfertigungsgrund. Hier kann neben der vertraglichen Verpflichtung oder der Einwilligung des Betroffenen auch das berechtigte Interesse des Verarbeiters herangezogen werden. Bei Letzteren handelt es sich aber um eine unbestimmte Rechtfertigungsnorm, die laufend durch Rechtsprechung weitergebildet wird. Eine Landwirtin bzw. ein Landwirt der Kunden- oder Mitarbeiterdaten verarbeitet sollte sich daher nicht leichtfertig auf dieses Grund berufen. Ansonsten steigt das Risiko eines Einspruchs gegen die Verarbeitung. Werden sensible Daten von Personen verarbeitet – wie etwa Gesundheitsinformationen – sieht Art 9 DSGVO ein noch strikteres Regime vor. In diesem Fall wird meist nur eine Einwilligung des Betroffenen zur Verarbeitung berechtigen. In der Landwirtschaft wird diese Kategorie von Informationen aber regelmäßig eine untergeordnete Rolle spielen.

Datenvermittlungsdienste (Art 10 ff DGA)

Der DGA sieht nicht bloß Regelungen für den Zugriff zu Informationen vor, die im Besitz von öffentlichen Institutionen sind, sondern führt daneben in seinen Art 10 ff auch sogenannte **Datenvermittlungsdienste** ein. Datenvermittlungsdienste sind besonders regulierte Intermediäre, die den Nutzerinnen bzw. Nutzern von Informationen eine sichere und vertrauenswürdig Umgebung bieten sollen, um Daten zum Austausch anzubieten.[87]

Die EU soll damit zur Vorreiterin einer datennutzenden Gesellschaft werden und den oftmals komplexen Vorgang des Informationsaustauschs zwischen verschiedenen Parteien vereinfachen und Transaktionskosten reduzieren.[88]

Gem Art 2 Z 11 DGA handelt es sich bei Datenvermittlungsdiensten um Dienste, die darauf abzielen, durch technische, rechtliche Mittel Geschäftsbeziehungen zum Zwecke des Teilens von Informationen zwischen Dateninhaberinnen/Dateninhabern und Datennutzerinnen/Datennutzern herzustellen. Dem Wortlaut folgend ist somit reines „Daten-Brokerage“ – bei dem gekaufte Informationen an Dritte weitergegeben werden – nicht von der Definition umfasst.[89] Vielmehr wird es sich bei Datenvermittlungsdienste um Plattformen handeln, auf denen Informationen zwischen Anbieter und Nachfrager ungehindert übermittelt werden können.

Datenvermittlungsdienste sind gem Art 11 DGA anmeldepflichtig. Die Dienstleistung darf somit erst angeboten werden, wenn die Anmeldung bei der zuständigen Stelle eingegangen ist. Ob eine Dienstleistung als Datenvermittlungsdienst zu bewerten ist, muss jedes Unternehmen selbst und auf eigenes Risiko beurteilen.[90] In Österreich ist bis dato auch noch keine zuständige Stelle festgelegt worden.

Obwohl die Einstiegshürde mit einer Meldung recht niedrig gehalten ist, sind für die Ausübung eines Datenvermittlungsdienstes umfangreiche Pflichten vorgesehen. So sind gem Art 12 lit a DGA Datenvermittlungsdienst etwa zur Neutralität zwischen Anbieter und Nachfrager verpflichtet. Demnach ist etwa die Aufbereitung von Informationen für eine der beiden Seiten untersagt. Eine Ausnahme besteht dabei nur für solche Bearbeitungen, die den Austausch der Information erleichtert.

---

87 *Dobner/ Scharl/ Zwinger*, Neues aus Brüssel, SozSi 2022, 142 (144).
88 ErwG 22 DGA.
89 *Hennemann/Von Ditfurth*, Datenintermediäre und Data Governance Act, NJW 2022, 1905 (Rn. 14).
90 *Gellert/Graef* TILEC Discussion Paper 2021-006, 9.

Gem Art 12 lit b ist auch die Kopplung des Datenvermittlungsdienstes an andere Leistungen des Unternehmens verboten. Kopplungsverbote finden sich üblicherweise im Wettbewerbsecht und gelten für besonders einflussreiche Unternehmen, die ansonsten ihre Marktstellung ausnutzen würden. Das generelle Kopplungsverbot für Datenvermittlungsdienste ist daher kritisch zu sehen. Man wird nämlich davon ausgehen können, dass nicht jeder Datenvermittlungsdienst automatisch sofort eine marktbeherrschende Stellung einnehmen wird.

Neben der Pflicht, angemessene Maßnahmen zur Interoperabilität mit anderen Datenvermittlungsdiensten zu treffen und einen diskriminierungsfreien Zugang zum Dienst zu gewährleisten, werden in Art 12 auch umfangrieche Überwachungs- und Sicherheitspflichten für die Datenvermittlungsdienste normiert. So müssen angemessene Maßnahmen getroffen werden, um die Weitergabe von rechtswidrigen Informationen zu verhindern. Diese Pflicht dazu führen, dass die altbekannte Diskussion über „Up-Load-Filter“ nun bei den Datenvermittlungsdiensten erneut entbrennt.

Zusammenfassend betrachtet können einheitliche Standards die Nutzung von Plattformen zum Austausch von Informationen zwar attraktiver machen, das besonders enge Regulierungskorsett des DGA läuft aber Gefahr Unternehmen von dieser Dienstleistung eher fernzuhalten. Hier wäre es zu begrüßen, wenn den zukünftigen Informationsvermittlern nicht nur Pflichten umgehängt, sondern auch gewisse Anreize geboten werden.[91]

Zusammenfassende Rahmenbedingungen eines Data Spaces „Smart Farming“

Die Ergebnisse der vorliegenden Untersuchung lassen sich als Rahmenbedingungen für einen Data Space „Smart Farming“ wie folgt zusammenfassen:

- **Kein Dateneigentum, aber immaterialgüterrechtlicher Schutz**
  - Die österreichische Rechtsordnung und auch der EU-Rechtsrahmen vermitteln keine absoluten Rechte an Daten und Information. Insofern besteht an unkörperlichen Daten kein sachenrechtliches Eigentum. Landwirtschaftliche Information kann jedoch dem Schutz des Urheberrechts oder des Geschäftsgeheimnisrechts unterliegen, wodurch ein gewisser Schutz und damit einhergehende disponible Vermögensrechte bestehen.

- **Datenschutz liefert nur begrenzte Datenhoheit**
  - Die DSGVO stärkt die Rechtsposition von natürlichen Personen im Zeitalter der Digitalisierung, ein Eigentum an Informationen vermittelt diese jedoch nicht. Mit Löschungs-, Änderungs-, oder Einschränkungsansprüchen kann zwar die Informationsverarbeitung eines Dritten maßgeblich beeinflusst werden – die Rechte haben jedoch primär Schutzcharakter und begründen für sich genommen keine disponiblen Vermögensrechte an personenbezogenen Daten.

[91] *Hennemann/Von Ditfurth,* Datenintermediäre und Data Governance Act, NJW 2022, 1905 (Rn. 30).

— **Geschäftsgeheimnisschutz liefert keine Datenhoheit**
  - Der Schutz von Daten als Geschäftsgeheimnis weist die geheime Information nicht ausschließlich dem Geheimnisinhaber zu. Dieser hat nur zivilrechtliche Ansprüche gegen bestimmte Formen des rechtswidrigen Erwerbs (iSd Überwindung des Geheimnischarakters) sowie der rechtswidrigen Nutzung und Offenlegung. Der Inhaber eines Geschäftsgeheimnisses hat jedoch keine Handhabe gegen andere Unternehmen, welche das Geheimnis eigenständig erarbeiten (zB durch eigenständige Versuche) oder durch ein zulässiges Analysieren von Produkten ("Reverse Engineering“) in Erfahrung bringen.

— **„Besitzer“ und „Inhaber“ iSd DGA sind nicht sachenrechtlich zu deuten**
  - Während im Data Governance Act vom Besitz an Daten gesprochen wird, ist im aktuellen Entwurf des Data Act der „Dateninhaber“ sogar ausdrücklich definiert. Beide Begriffe lassen eine gewisse rechtliche Zuordnung von Informationen zu Personen vermuten. Tatsächlich knüpfen beide Regelungen jedoch ausschließlich an den faktischen Zugriff auf Daten und nehmen keinen Bezug zur rechtlichen Verbindung.

— **Data Act: voller Zugriff – kleiner Rahmen**
  - Der aktuelle Entwurf des Data Act räumt Personen weitreichende Zugangsrechte zu Informationen ein. Da die Regelung aber nur auf solche Informationen anzuwenden ist, die durch die Nutzung von „vernetzten Produkten“ und damit “verbundenen Diensten“ entstehen, ist der tatsächliche Anwendungsbereich stark begrenzt.

— **Data Act: Access by Design (im besten Fall)**
  - Grds verpflichtet der Data Act künftig, „vernetzte Produkte“ und damit “verbundene Dienste“ so zu gestalten, dass die Nutzerin bzw. der Nutzer unmittelbar auf die erhobenen Informationen zugreifen kann. Im Fall von Umsetzungsschwierigkeiten kann diese Pflicht aber durch eine Zurverfügungstellung der Informationen auf Anfrage ersetzt werden kann. Dabei besteht das Risiko, das verpflichtete Unternehmen vorschnell die Unmöglichkeit eines unmittelbaren Zugangs einwerfen.

— **Data Act: Risiko von Normkonflikten**
  - Kommt es zu Anwendung der Zugangs- oder Weitergaberechte des Data Act Entwurfs, müssen in jeden Fall auch andere Datenschutzbestimmungen berücksichtigt werden. Gerade bei erhobenen Informationen, die einen Personenbezug auf Dritte aufweisen, kann der ein Konflikt mit den Verarbeitungsvorschriften der DSGVO entstehen.

— **Datenvermittlungsdienste: Viele Pflichten – keine Anreize**
  - Die neu geschaffenen Datenintermediäre – sogenannte Datenvermittlungsdienste – sind durch den Data Governance Act eingeführt worden und sollen in Zukunft für einen regen Austausch von Informationen innerhalb der EU sorgen. Durch eine Flut an Verpflichtungen verliert diese Tätigkeit aber stark an Attraktivität.

Handlungsempfehlungen und -spielräume

Zusammenfassend lassen sich – unbeschadet der im Expertenpapier detailliert adressierten Maßnahmen – aus rechtswissenschaftlicher Sicht folgende Handlungsempfehlungen ableiten:

#1 Schulung und Bildung: Landwirtinnen und Landwirte sollten über ihre Rechte und die Bedeutung der Daten, die sie produzieren oder nutzen, informiert werden. Aufgrund der weitreichenden zivilrechtliche Handlungsräume bei der Gestaltung von Verträgen über Daten oder den Zugang zu Information, bedarf es weniger einer gesetzlicheren Regulierung als vielmehr eines Capacity Buildings unter den Landwirtinnen und Landwirten.

#2 Förderung von Transparenz: Ungeachtet des Erfordernisses, das Verständnis von Landwirtinnen und Landwirten in Bezug auf ökonomische und rechtliche Aspekte der Datenwirtschaft zu schärfen, sind transparente (klare und verständliche) Verträge erforderlich, sodass Landwirtinnen und Landwirte überblicken können, welche Rechte diese in Bezug auf Daten oder Informationen einräumen oder erhalten. Ein solcher Transparenzgedanke ist ansonsten zwar konsumentenschutzrechtlich geprägt, erscheint aber angesichts der vielfach vorliegenden Informationsasymmetrie oder des wirtschaftlichen Ungleichgewichts der Marktteilnehmer in diesem Kontext angezeigt.

#3 Einführung von Standardverträgen: Das Fehlen eines eigenen, gesetzlich detailliert beschriebenen Vertragstypus für Transaktion betreffend Daten oder Informationszugänge überrascht angesichts der Bedeutung für die Wirtschaft. Durch eine gesetzliche Definition und Ausgestaltung – die freilich nicht zwingend (jedenfalls nicht vollständig zwingend) ist – eines neuen Vertragstypus würde ein gesetzlich umrissener „Standardvertrag“ entstehen, der allen Marktteilnehmerinnen bzw. Marktteilnehmern (damit auch den Landwirtinnen und Landwirten) als Benchmark für einen fairen und angemessenen Vertrag in Zusammenhang mit Daten und Information dienen kann.

#4 Gesetzliche Klarstellungen vornehmen: Es bedarf einer präzisen, gesetzlichen Festlegung, welche Rechte und Pflichten im Zusammenhang mit Daten und dem Zugang zu Informationen bestehen. Dies beinhaltet eine klare Definition des Daten- und Informationsbegriffs nicht nur in Sondergesetzen, sondern auch im allgemeinen Zivilrecht. Zudem sollte klargestellt werden, unter welchen Voraussetzungen Daten oder Informationen geteilt, verkauft oder anderweitig kommerziell genutzt werden dürfen („Datenvertragsrecht“). Gesetzliche Klarstellungen schaffen Rechtssicherheit für alle Marktteilnehmerinnen bzw. Marktteilnehmer und somit einen stabilen Rahmen für wirtschaftliche Aktivitäten – auch im landwirtschaftlichen Bereich.

#5 Datenvertragsrecht statt „Dateneigentum“: In der rechtlichen Diskussion um Daten und Information steht vielfach die Frage im Vordergrund, ob Daten oder Information „eigentumsfähig“ sind oder sein sollen, was letztlich die Schaffung neuer dinglicher Rechte an Daten oder Information erfordern würde. Doch die Schwächen eines solchen Ansatzes sind evident und zeigen sich bei der Konturierung eines solchen Rechts sowie bei der Frage der originären Allokation, wenn – wie im Regelfall – mehrere Akteure an der Erstellung, Nutzung und Verarbeitung von Daten beteiligt sind. Daher sollte der Fokus weniger auf einem möglichen „Dateneigentum“ liegen, sondern vielmehr auf einem „Datenvertragsrecht“. Dieses wäre darauf auszurichten, die verschiedenen Interessen und Rechte der Beteiligten im Rahmen vertraglicher Beziehungen auszugleichen. Es sollte – unter Beachtung der Vorgaben des Unionsrechts – einen klaren Rahmen dafür schaffen, wie Daten in verschiedenen Kontexten genutzt, geteilt und verwertet werden können.

Anhang: Verzeichnisse

Abkürzungsverzeichnis

ABGB ..... *Allgemeines Bürgerliches Gesetzbuch*
ABl ..... Amtsblatt
Abs ..... *Absatz*
AEUV ..... *Vertrag über die Arbeitsweise der EU*
Art ..... Artikel
bspw ..... *beispielsweise*
DA ..... *Data Act*, *Data Act*
Entw ..... Entwurf
ErwG ..... Erwägungsgrund
EuGH ..... *Europäischer Gerichtshof*
ff ..... *fortfolgende*
FMS ..... *Farm Management Informationssystem*
gem ..... *gemäß*
grds ..... *grundsätzlich*
idF ..... *in der Fassung*
idR ..... *in der Regel*
ieS ..... *im engeren Sinn*
iSd ..... *im Sinne des*
iVm ..... *in Verbindung mit*
iZm ..... *im Zusammenhang mit*
KartG ..... *Kartellgesetz*
LMH ..... *Landmaschinen des Herstellers*
LMV ..... *Landmaschinenverleiher*
LW ..... *Landwirtschaftlicher Betrieb*
MaW ..... *mit anderen Worten*
OGH ..... *Oberster Gerichtshof*
Rn ..... *Randnummer*
Rz ..... *Randziffer*
StGG ..... *Staatsgrundgesetz*
StRsp ..... *ständige Rechtssprechung*
UrhG ..... *Urheberrechtsgesetz*
vgl ..... *vergleiche*

Abbildungsverzeichnis

Abbildung 1: Exemplarisches Szenario – Akteure und Interaktion 4
Abbildung 2: Information, Daten und Datenträger 7