Die „dunkle Materie“ des Datenschutzes – Was passiert eigentlich im Backend?

[19.11.2021]

Von: Dr. Axel-Michael Wagner und Lukas Fleischer

Datenschutzrecht kann man aus verschiedenen Perspektiven betrachten. Eine davon betrifft die Frage, welche personenbezogenen Daten von Unternehmen wie verarbeitet werden. Jedes Unternehmen verarbeitet Daten über betroffene Personen, seien es Beschäftigte, Kunden, Ansprechpartner anderer Unternehmen oder sonstige Personen, die für das Unternehmen im Zusammenhang mit einer Geschäftstätigkeit relevant sind. Um diese Datenverarbeitung, die durchaus einen wesentlichen und strategischen Teil der Geschäftsaktivitäten ausmachen kann, soll es im Folgenden gehen. Was dort im Einzelnen geschieht, ist häufig von außen kaum transparent einsehbar, und die Verarbeitungstätigkeit in den „dunklen Server-Hallen“ der Unternehmen sieht sich auch rechtlich häufig im Dunkeln. Worüber müssen Unternehmen nachdenken?

Was will Datenschutz von den verantwortlichen Unternehmen?

Schon immer haben Informationen die „Menschenwelt“ gesteuert und waren insoweit auch eine Art „Rohstoff“ bei der Entwicklung von Gesellschaft und Wirtschaft. Und schon immer wurden – in antiken Staatsgebilden und natürlich im Militär – Informationen systematisch erhoben und zusammengeführt, um eine Vorstellung von der Realität „da draußen“ besser vermitteln zu können. Neben dem informationsverarbeitenden System Mensch, der solche Informationen erhebt und verarbeitet, trat in der zweiten Hälfte des 20. Jahrhunderts die elektronische Datenverarbeitungsanlage „EDV“. Informationen jeder Art können in diese „Informationstechnologie“ eingespeist, in Datenbanken strukturiert und in beliebiger Weise miteinander verknüpft und an andere Systeme übertragen werden. Eine wesentliche Gefahr, der das Datenschutzrecht begegnen will ist, dass solche Daten, wenn sie sich auf natürliche Personen beziehen, ohne Wissen und Zustimmung der betroffenen Person in den eingangs apostrophierten dunklen Server-Hallen ein Eigenleben entfalten und die Ergebnisse solcher Operationen dann gegen die betroffene Person gewendet werden. Schon die Angst davor, dass so etwas passieren könnte, hat Einfluss auf das Verhalten von Menschen. Jeder, der im Unternehmensumfeld mit personenbezogenen Daten hantiert, sollte diesen Gedankengang verstehen, unabhängig davon, ob er ihn persönlich teilt.

Die Möglichkeiten der modernen Datenverarbeitung führten 1970 zum ersten Datenschutzgesetz und 1983 zu einer Entscheidung des Bundesverfassungsgerichts, das ein „Recht auf informationelle Selbstbestimmung“ prägte. Beides reflektierte die Möglichkeiten der modernen Datenverarbeitung als Paradigmenwechsel in der Informationsverarbeitung, da die neuen Automaten Informationen wesentlich schneller, umfänglicher und echtzeitvernetzter verarbeiten konnten. Kann aber der einzelne Mensch in einer solchen Umgebung nicht über die Preisgabe und Verwendung seiner Daten bestimmen, wird er sich überwacht fühlen und aus Vorsicht anders agieren, was ihn beschränkt und in der Folge das Gemeinwohl beeinträchtigt. Seinerzeit bezog sich diese Sorge allumfassender „Gläsernheit“ zunächst auf den Staat als „Datenkrake“; nicht umsonst stammt die verfassungsgerichtliche Entscheidung aus dem Kontext der Volkszählung. Später kamen dann auch noch die Unternehmen der Privatwirtschaft hinzu, deren Geschäftsmodell die automatisierte Verarbeitung personenbezogener Daten umfasst. Seien es auch nur die Daten der eigenen Beschäftigten und unternehmensbezogene Kontaktdaten von Beschäftigten anderer Unternehmen. Auch die Datenverarbeitung durch Unternehmen der Privatwirtschaft kann – das zeigen die modernen Social-Media-Giganten eindrucksvoll – zu einer Durchleuchtung eines zunehmend gläsernen Betroffenen führen und sich in negativen Folgen für ihn niederschlagen, und sei es auch nur in Form unerwünschter Werbungsansprache.

Soll der Einzelne also autonom über das Schicksal seiner Daten bestimmen können, muss er einerseits wissen, was mit diesen Daten passiert. Und andererseits muss er die Möglichkeit haben zu steuern, was mit diesen Daten passiert. Nun kann das Datenschutzrecht aber schlecht Staat und Unternehmen zu Treuhändern von Daten Einzelner erklären, die mit den Daten weisungsabhängig umzugehen haben, schon allein deswegen, weil dies auf individuelle Kommunikation und „Verhandlungen“ zwischen der betroffenen Person und dem Verantwortlichen hinauslaufen würde, was im heutigen Massendatenverkehr unmöglich umzusetzen wäre. Auch im Vertragsrecht konnte man seit jeher als Verbraucher kaum mit einem Unternehmen als Vertragspartner verhandeln; dazu war man schlicht zu unwichtig, das Produkt oder die Dienstleistung zu standardisiert und das subjektive Verlagen nach Ware oder Dienstleistung oder Partizipation größer als der rebellische Wunsch, die „Macht der Verbraucher“ zu entfesseln (meist bleibt dies dann auch nur eine Rebellion des Einzelnen). Dies führte in den 1970er-Jahren zum gesetzlichen Verbraucherschutzrecht, das zwischenzeitlich ein wichtiger Bestandteil des Zivilrechts ist und die Privatautonomie – hier in Form der Möglichkeit, ein Machtgefälle bei der Vertragsverhandlung zu Lasten von Verbrauchern auszunutzen – erheblich begrenzt.

Auch bzw. erst recht im Datenschutz sieht sich der Betroffene keinem Menschen mehr gegenüber, sondern einem (Verarbeitungs-) „System“, das entsprechend seiner

Programmierung die Regeln setzt – ein Umstand, der oft schlagwortartig auch als „code as law" bezeichnet wird. Facebook mag aus Sicht von „Otto Normalfacebook-Usern" zwar einen (!) sehr prominenten Mitarbeiter haben, dessen Gesicht hin und wieder in der Presse erscheint. Aber im Grunde ist Facebook eine riesige Maschine und diejenigen, die diese Maschine im Einzelnen konzeptionieren und programmieren, treten gegenüber dem Nutzer nicht als Menschen in Erscheinung. Und selbst wenn einem in einer Bank noch ein Mitarbeiter in Fleisch und Blut gegenübersteht, kolportiert er doch meist nur das, was „der Computer" zum Kunden weiß und über den Kunden entschieden hat. Mit einem programmierten System lässt sich schlecht verhandeln. Eine Ein- oder Ausgabe, die nicht vorgesehen wurde, kann nicht verarbeitet oder generiert werden.

Man könnte daher zu dem Schluss kommen, dass Datenschutzrecht in erster Linie Verbraucherschutzrecht (einschließlich: Arbeitnehmerschutzrecht) ist und Situationen asymmetrischer Machtverteilung regulieren soll. Wie im Recht der Allgemeinen Geschäftsbedingungen schreibt der Gesetzgeber dann „Grenzen der Benachteiligung" vor zu dem Zweck, die abhanden gekommene Privatautonomie (Selbstbestimmung) des Verbrauchers bei der Vertragsverhandlung – heutzutage ist für viele eine Facebook-Mitgliedschaft mindestens so wichtig wie der Kauf von Brot – durch „zwingendes Recht" zu ersetzen. Nicht umsonst ist in diesem Zusammenhang von einem „notwendigen Paternalismus" des Staates die Rede: Wenn der Bürger von der marktkonzentrierten Übermacht von Großkonzernen und/oder von der zwingenden Logik einer „Plattform" überrollt zu werden droht, muss der (selbst von der faktischen Entwicklung meist überraschte) Staat altväterlich die Dinge irgendwie „zurechtrücken".

Dem scheint zwar entgegenzustehen, dass die DSGVO als Legitimationsgrund für Datenverarbeitungshandlungen zuerst die Einwilligung nennt. Der damit propagierte Schwerpunkt des Datenschutzrechts auf Selbstbestimmung ist aber angesichts der oben dargestellten Strukturen ein Potemkinsches Dorf. In der Realität tritt vielmehr eine gleichgültige Überforderung der betroffenen Person durch ständige Akzeptanz seitenlanger Einwilligungserklärungen ein. Einerseits ist vielen schlicht gleichgültig, was mit ihren Daten passiert, d. h. sie „klicken auf alles", nur um weiterzukommen. Andererseits sieht man in der konkreten Situation auch gar keinen anderen Ausweg als einzuwilligen, weil die begehrte Ware, Dienstleistung oder Information mit der Erteilung „irgendeiner" Einwilligung verknüpft ist. Eine Verhandlung der Einwilligung ist nicht möglich; die Wahlmöglichkeiten beschränken sich allenfalls noch, wie bei Cookies, darauf, an wen Daten weitergegeben werden, aber was mit den Daten im Einzelnen – wiederum von einem System vorgegeben – passiert, lässt sich nicht aushandeln (und ist meist auch nicht transparent). Die selbstbestimmte Einwilligung ist also häufig gar nicht selbstbestimmt. Ob bzw. wie eine Einwilligung in eine im Detail hochkomplexe Datenverarbeitung über viele Systeme hinweg überhaupt selbstbestimmt möglich wäre,

wird dabei meist nicht hinterfragt. Folglich setzt das Datenschutzrecht eigene, normative Grenzen und gibt vor, wann eine betroffene Person das ihr zugedachte Selbstbestimmungsrecht überhaupt noch freiwillig ausübt und wann sie – mutmaßlich – nicht selbstbestimmt (einschließlich „nicht genügend informiert“) handelt und vor sich selbst geschützt werden muss.

Ein Teil des Datenschutzrechts will also den Betroffenen vor seiner eigenen Gleichgültigkeit und Überforderung schützen. Einwilligungserklärungen des erschöpften Subjekts werden anhand einer „wertenden Betrachtung“ neudeutsch „overruled“. Ein solches „Overruling“ findet insbesondere in (vermuteten) Abhängigkeits- oder Zwangsentscheidungslagen statt sowie dann, wenn die Aufklärung des Betroffenen über die anstehende Datenverarbeitung für einen „mittelaufmerksamen Verbraucher“ nicht mehr nachvollziehbar zu sein scheint (was natürlich Richter rückschauend für alle Betroffenen pauschal entscheiden). Die damit einhergehende Rechtsunsicherheit über die Wirksamkeit der Einwilligung rückt damit für die Verantwortlichen ersatzweise die Möglichkeit in den Vordergrund, berechtigte Unternehmensinteressen mit den typisiert-abstrakten (also mutmaßlichen) Interessen eines fiktiven Betroffenen abzuwägen und so die tatsächlich gegebene Einwilligung durch eine „mutmaßliche Einwilligung“ zu ersetzen. Damit entfällt vordergründig das für den Betroffenen „lästige Kreuzchen“ und die Gefahr, dass sich doch einmal jemand abwendet (statt einwilligt). Einer – virtuell – „vor dem Verantwortlichen sitzenden Person“ wird dann anstelle einer direkten Frage nach Einwilligung eine mutmaßliche Einwilligung, die auf einer Abwägung beruht, die (ausgerechnet) vom „Widerpart“ der betroffenen Person vorgenommen wurde, untergeschoben. Der aufgrund dieser etwas absurden Situation von der Rechtsprechung vor Inkrafttreten der DSGVO propagierte „Vorrang der Einwilligung“ ist zwischenzeitlich seltsamerweise etwas aus dem Blickfeld geraten und man geht in der Praxis überwiegend von einer Gleichrangigkeit insbesondere von Einwilligung und Interessenabwägung als Legitimationsgrundlagen aus.

Ein anderer Teil des Datenschutzrechts will den Betroffenen über das Schicksal seiner personenbezogenen Daten „da draußen“ informieren, als wäre jedes einzelne Datum mit einem GPS-Tracker und einer Helmkamera mit Live-Übertragung ausgestattet, die in „kritischen“ Situationen aktiviert werden. Diese kritischen Situationen sind möglicherweise – dazu noch unten – die Übermittlung an einen anderen Verantwortlichen, in jedem Fall aber die Zweckänderung. Daneben sind zwischenzeitliche Empfänger personenbezogener Daten, die vom ursprünglichen Verantwortlichen weiterübermittelt wurden, von Berichtigungen, Löschungen und Sperrungen zu informieren. So müsste eigentlich jeder Verantwortliche jedes Datum „monitoren“ und immer mal wieder auch Nachrichten an andere „Beteiligte“ absetzen, um den Status des als Kopie weiter verbreiteten Datums mit dem Original zu

synchronisieren. Die weithin unsichtbare Verarbeitung von Daten in den sprichwörtlichen dunklen Server-Hallen soll durch solche Mechanismen ein wenig erhellt und die verschiedenen Verantwortlichen, die sich Daten gegenseitig „zuschieben", miteinander vernetzt werden. Das ist auch vor dem Hintergrund zu sehen, dass später grundsätzlich „jeder an einer Verarbeitung beteiligte Verantwortliche" für eine datenschutzwidrige Verarbeitung haftet, soweit er nicht ausnahmsweise nachweisen kann, „in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich" gewesen zu sein (Art. 82 DSGVO).

Sowohl die „Mitteilungen über Daten" als auch die „Bewertung von Freiwilligkeit und Mutmaßung der Interessen Dritter" bedeuten für datenverarbeitende Unternehmen allerdings einen erheblichen Aufwand und eine erhebliche und vermutlich nie ganz ausräumbare Rechtsunsicherheit, und zwar gleichermaßen bei der internen Bewertung und Dokumentation von Konzepten als auch bei deren Umsetzung. Diese in neueren Gesetzen weiter zunehmende Rechtsunsicherheit wird euphemistisch mit dem Konzept des „self-assessment" umschrieben: Nicht der Gesetzgeber sagt, was im Einzelnen erlaubt und verboten ist, sondern er stellt sehr abstrakte, fast schon kryptische Generalklauseln und Zielvorstellungen (Redlichkeitsprinzipien) auf und gibt den „Verantwortlichen" vor, eine „Risikoabwägung" oder „Datenschutz-Folgenabschätzung" durchzuführen, in welche maßgeblich die Interessen der eigenen Kunden, „Targets" und Beschäftigten des Verantwortlichen einfließen sollen. Warum sollte nun ein Verantwortlicher in diesem Rahmen auf den Gedanken kommen und für sich dokumentieren, dass die Masse der „Targets" beispielsweise versendete Werbung als belästigend empfinden könnte? Natürlich wegen der Androhung drakonischer Strafen, die sich materialisieren, wenn später herauskommt, dass man nicht genug „gegen seine eigenen Interessen gedacht" hat. Der so erzwungene Aufwand im Unternehmen bei der Konzeption und Umsetzung von Datenverarbeitungen – unabhängig von Größe und Geschäft des Unternehmens – wurde nie auch nur annähernd in einem parlamentarischen Verfahren erkannt, geschweige denn diskutiert. Niemand weiß, welcher Aufwand gesamtwirtschaftlich seit Inkrafttreten der DSGVO – entgegen der in der Rückschau „niedlichen" Kostenschätzungen im Rahmen der damaligen Rechtsfolgenabschätzung – in (unternehmensinterne) Projekte zur Anpassung komplexer IT-Landschaften geflossen ist. Das soll nicht heißen, dass es diesen Aufwand nicht hätte geben sollen, sondern, dass die Chance verpasst wurde, die DSGVO anders zu formulieren, wenn man solchen immensen Aufwand vorhergesehen hätte.

Wie gehen Verantwortliche mit den Vorgaben um?

Nun kann das Recht zwar etwas vorschreiben, aber das garantiert noch lange nicht, dass sich die Welt auch tatsächlich so entwickelt. Die Möglichkeiten, Daten wie natürliche Rohstoffe „auszubeuten", also ihren maximalen ökonomischen Nutzwert herauszuziehen,

werden immer größer, und damit wachsen bekanntermaßen auch die Begehrlichkeiten der Unternehmen. Täglich werden mehr Daten erhoben, verknüpft, übertragen und Betroffene mit aus ihren Daten gezogenen Schlussfolgerungen konfrontiert – in welcher Weise und mit welchen „Folgeschäden" für die Betroffenen auch immer. In der realen Datenwelt regiert schon lange das „anything goes", gepaart mit einer kapazitätsbedingt niedrigen Kontrolldichte seitens der Aufsichtsbehörden. Dem wirkt jedoch neuerdings im Fahrwasser der DSGVO steigende „Awareness" entgegen: Es gibt mehr und mehr betroffene Personen, Aktivisten, Verbraucherschutzverbände, Whistleblower und desgleichen mehr, die sich über das, was mit den Daten passiert, aktiv informieren und bisweilen gerichtliche Klärung suchen (die dann oft in niedrigen Instanzen „steckenbleibt"). Und diese Awareness wiederum führt mutmaßlich zu mehr verantwortlichen Unternehmen, die sich über das, was in ihren Server-Hallen abspielt, ob Kerngeschäft oder „trial and error" der Marketing-Abteilung, vertiefte datenschutzrechtliche Gedanken machen. Auch wenn das – wie „Compliance" allgemein – Geld kostet, was natürlich vor allem den Mittelstand verdrießt.

Dabei stellt sich schnell heraus, dass die DSGVO aufgrund der oben angesprochenen, (bewusst) abstrakten Formulierungen viele Graubereiche enthält, die teils bewusst ausgestaltet, teils im Gesetzgebungsverfahren nicht gesehen wurden. Abseits der glasklaren Fälle ist die DSGVO also im konkreten Fall eine schlechte „Guidance". Dies gilt leider auch für die einzig verbindlichen Entscheidungen des Europäischen Gerichtshofes, die (wie jede Gerichtsentscheidung) konkrete Fälle punktuell beleuchten (leider teils mit unverständlichen Begründungen) und nicht (wie ein Gesetz) den Anspruch haben, ein in sich stimmiges Gesamtsystem zu etablieren. Jeder Jurist weiß, dass eine Fallgestaltung, die „einen Millimeter neben einer Präzedenzentscheidung" liegt, möglicherweise im Ergebnis genau andersherum gesehen werden muss – wir werden hiervon noch Beispiele sehen. Außerhalb der DSGVO und der EuGH-Entscheidungen kann hingegen jede weitere „Guidance" keine Verbindlichkeit für sich in Anspruch nehmen. Die Antwort wird in diesem großen Bereich des „known unknown" davon abhängen, zu welcher Interessengruppe derjenige gehört, den man befragt.

Für die Unternehmen rückt daher gerade in den Graubereichen der DSGVO – das mag man gut finden oder nicht – das Thema Entdeckungswahrscheinlichkeit in den Vordergrund. Insbesondere bei Auskunftsersuchen steht das Unternehmen vor der Frage, ob Daten, über die man Auskunft erteilen müsste, „nicht besser schon gelöscht worden wären", sodass man das (ggf. auch nur teilweise) Löschen noch schnell außerplanmäßig vor der Auskunftserteilung nachholt. Dasselbe könnte man anlässlich der Herkunft oder der Verarbeitungszwecke tun wollen, wenn diese nicht im Einklang mit Pflichthinweisen an den Betroffenen standen oder sich datenschutzrechtlich als zweifelhaft erweisen könnten. Im Extremfall kann das soweit gehen, dass ein Unternehmen bestreitet,

überhaupt Daten über eine Person zu haben, weil es sich die Konsequenzen einer entsprechenden Auskunftserteilung ausmalen kann. Der Nachweis des Gegenteils ist dann im Wesentlichen unternehmensinternen Whistleblowern vorbehalten. Denn spektakuläre „Strafexpeditionen" der Datenschutzbehörden in verantwortlichen Unternehmen, ggf. in Begleitung der Staatsanwaltschaft (auf Grundlage der Datenschutzstraftaten in § 42 BDSG), zur forensischen Überprüfung der Richtigkeit von gegebenen Auskünften sind bislang nicht bekannt. Das mag auch daran liegen, dass die Graubereiche der DGSVO natürlich den Aufsichtsbehörden bekannt sind und sich ins Strafrecht fortsetzen. Da konzentriert man die knappen Kapazitäten lieber auf die klareren Fälle. Mit so viel Unbestimmtheit und Vollzugsdefizit versehen wird die DSGVO eher zu einem lästigen mobilen Blitzer auf der Autobahn, dessen Blitz einfach für „Pech" gehalten wird und dem man danach – mit offenem Ausgang – einen Messfehler vorhalten kann. Diese faktische Situation kann man politisch gut finden oder nicht, aber wenn jeder Datenschutzverstoß – was immer das im Detail ist – konsequent aufgedeckt und verfolgt werden sollte, müsste man wohl die gesamte Bevölkerung zu Mitarbeitern der Datenschutzaufsichtsbehörden machen.

Das Dilemma der Graubereiche kann auch der nachfolgende Beitrag nicht auflösen. Hier soll es darum gehen, die Sensibilität für das zu erhöhen, was zu bedenken ist, wenn unternehmensintern mit personenbezogenen Daten „hantiert" wird. Mit „Hantieren" ist nicht das Erheben, Speichern (d. h. „Vor-sich-hin-schlummern") und Löschen von Daten gemeint, das in großem Maßstab und bei minimalen Speicherkosten zu ungenutzten Datenfriedhöfen führt, die man ungerne aufräumt, weil man nie weiß, wofür man das noch einmal brauchen könnte (ultimatives Argument: eine Betriebsprüfung könnte das noch einmal sehen wollen). Es geht auch nicht um die einfache Operation, eine E-Mail-Adresse eines Betroffenen aus einer Datenbank auszulesen und einen vorgefertigten E-Mail-Text an diese Adresse zu schicken. Vielmehr steht die Arbeit mit der „Knetmasse Daten" im Vordergrund, man könnte ökonomisch von der Daten-Wertschöpfungskette sprechen (Einkauf von Rohmaterial, eigene Wertschöpfung und gewinnbringende Nutzziehung, z. B. durch Verkauf oder „Anwendung der Erkenntnisse auf den Betroffenen").

Daten als Arbeitsmaterial

Zwei Beispielsfälle bilden den Einstieg bei der Beantwortung der Frage, wie Unternehmen inhaltlich im Backend mit Daten hantieren. In einem Fall in Österreich hatte die dortige Post Millionen von Datensätzen von Betroffenen um eine errechnete „politische Affinität" angereichert, also anhand der vorhandenen Daten (Alter, Adresse etc.) eine statistische Wahrscheinlichkeit der politischen Vorlieben ermittelt. Die Betroffenen wussten dies nicht und die Daten wurden, gefiltert nach dieser mutmaßlichen Affinität, politischen Parteien

für Werbezwecke zur Verfügung gestellt. Die Bußgeldentscheidung der österreichischen Datenschutzaufsicht wurde zwar vom österreichischen Bundesverwaltungsgericht im Dezember 2020 wegen eines Formfehlers aufgehoben, was aber nichts daran ändert, dass das Gericht die Datenschutzwidrigkeit des Vorgehens feststellte. Man kann dieses Vorgehen abstrakt so beschreiben, dass vorhandene Daten über den ursprünglichen unmittelbaren Erhebungszweck (Sicherstellung der postalischen Erreichbarkeit etc.) hinaus um Erkenntnisse „angereichert" werden und diese zusätzlichen Erkenntnisse sich irgendwann „auf den Betroffenen auswirken". Der Fall kam auf, nachdem eine Investigativ-Plattform bei der Post mehrere Auskunftsbegehren eingereicht hatte und die daraufhin erteilte Auskunft als weitere „Excel-Spalte" bzw. Datenbankfeld auch die errechnete Parteizugehörigkeit mitgeliefert hatte. Es waren also bemerkenswerterweise nicht die Empfänger der Parteiwerbung, die sich über die Verwendung bzw. Herkunft der Daten beschwert hatten.

Allgemein gesprochen, nutzen Unternehmen Daten, ggf. in Verbindung mit anderen Daten, dazu, Erkenntnisse über die betroffene Person zu gewinnen. Dies umfasst beispielsweise die Ermittlung persönlicher Präferenzen (oder Empfänglichkeit) im Bereich personalisierter Werbung und Angebote, die Anwendung von „KI-Algorithmen" auf Daten zur Entdeckung von struktureller Ähnlichkeiten oder Auffälligkeiten sowie die unternehmensinterne Verknüpfung (Anreicherung) von Daten aus verschiedenen Quellen für „Datensynergieeffekte". Diese Bereiche überlappen sich erheblich bzw. sind im Kern nur verschiedene Perspektiven auf ähnliche Auswertungsmöglichkeiten.

Die Entscheidung des österreichischen Bundesverwaltungsgerichts zeigt zunächst, dass die dadurch gewonnenen zusätzlichen Daten über eine Person auch dann, wenn sie nur „synthetisiert" wurden, also letztlich nicht mehr Informationsgehalt haben als die Ausgangsdaten (d. h. jeder, der die Ausgangsdaten hat, könnte denselben Erkenntnisgewinn verbuchen), ihrerseits personenbezogene Daten sind. Im Regelfall ist daher davon auszugehen, dass diese zusätzlichen Daten durch die „Errechnung" aus anderen (zumindest zum Teil personenbezogenen) Daten „erhoben" werden und damit eine Pflichtinformation an den Betroffenen notwendig machen (Art. 14 DSGVO). Diese Pflichtinformation muss insbesondere die Datenkategorie, den Verarbeitungszweck, die Rechtsgrundlage, die Empfänger und ggf. ein berechtigtes Interesse beschreiben. Eine Beschreibung der bei der Erhebung angewandten „Faustformeln" (in der Informatik: Heurismen) bzw. Algorithmen hingegen selbst, anhand derer die zusätzlichen Daten mehr oder weniger gut „erraten" wurden, gegenüber der betroffenen Person sieht die DSGVO nur für den Fall vor, dass anhand dieser Daten eine Entscheidung getroffen wird, „die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt" (Art. 22 Abs. 1 DSGVO). Ob diese Voraussetzung vorliegt, ist in der Praxis häufig schwer zu beurteilen, und auch, wie die dann dem Betroffenen zur Verfügung zu

stellenden „aussagekräftigen Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person“ genau aussehen müssen.

Natürlich können diese Pflichtinformationen auch schon bei der ursprünglichen Erhebung der „Ausgangsdaten“ mitgeteilt werden, wenn die Pflichtinformationen über die zusätzlich generierten Daten zu diesem Zeitpunkt schon feststehen. In der Praxis fällt Unternehmen jedoch bisweilen erst nach der Erhebung von Ausgangsdaten ein, welche Erkenntnisse sie mit bzw. aus diesen noch gewinnen könnten. Dann wird man sich die Frage stellen müssen, ob die Ausgangsdaten, die später für die Ermittlung weiterer Daten herangezogen wurden, eben diesem Zweck überhaupt von Anfang an dienen sollten. Wurden Daten etwa zu dem Zweck erhoben, diese für eine Aufrechterhaltung des Kontakts zu nutzen, so würde sich die Heranziehung dieser Daten für die Ermittlung einer Präferenz etc. möglicherweise als Zweckänderung darstellen. Dies würde neben der Durchführung und Dokumentation eines „Zweckkompatibilitätstests“ eine „Zweckänderungsmitteilung“ an den Betroffenen notwendig machen. Man kann sich als betroffene Person derartiger Datenverarbeitung – diese betroffene Person kann bzw. dürfte ja jede Bürgerin und jeder Bürger sein – ausmalen, wie viele Pflichthinweise und Mitteilungen man da eigentlich jeden Tag bekommen sollte, aber tatsächlich nicht bekommt. Von der Notwendigkeit einer dokumentierten Datenschutz-Folgenabschätzung wollen wir hier noch gar nicht sprechen.

In einem zweiten Fall hatte ein Rechtsanwalt Werbe-E-Mails für Kinder-FFP2-Masken bekommen und Schadensersatz vom Versender verlangt. Er habe diese Werbemails als ärgerlich und belästigend wahrgenommen. Das Amtsgericht Pfaffenhofen vollzog in einem Urteil vom September 2021 die vom Versender (implizit) vorgenommene Interessenabwägung nach und bezeichnete das Interesse des Versenders an Direktwerbung deswegen als nachrangig, weil der Versender (bisher) in keinerlei Beziehung zum Adressaten stand. Das Gericht sprach 300 Euro Schadensersatz zu und führte aus: *„Der Schaden kann auch bereits etwa in dem unguten Gefühl liegen, dass personenbezogene Daten Unbefugten bekannt geworden sind, insbesondere wenn nicht ausgeschlossen ist, dass die Daten unbefugt weiterverwendet werden, auch bereits in der Ungewissheit, ob personenbezogene Daten an Unbefugte gelangt sind. Unbefugte Datenverarbeitungen können zu einem Gefühl des Beobachtetwerdens und der Hilfslosigkeit führen, was die betroffenen Personen letztlich zu einem reinen Objekt der Datenverarbeitung degradiert“*. Die Beklagte hatte argumentiert, sie habe die E-Mail-Adresse „frei zugänglich“ vorgefunden, nämlich über eine Branchenbuch-Website. Um die Dimension der Entscheidung zu verstehen, muss man sich die Zahl der Fälle, in denen tagtäglich Ähnliches geschieht, vor Augen halten. Der Fall dürfte eigentlich auch hier nicht aufhören, sondern man müsste als Betroffener – wenn schon, denn schon – die gesamte

Datenverarbeitungskette bis zur ursprünglichen Erhebung der Daten „quer durch die dunklen Server-Hallen“ zurückverfolgen und jedes Glied der Kette auf Schadensersatz in Anspruch nehmen, wie es Art. 82 Abs. 2 DSGVO vorsieht.

Man kann diese Fallgestaltung abstrakt so beschreiben, dass Daten ohne Wissen des Betroffenen „von irgendjemandem“ erhoben und zwischen verschiedenen Akteuren „verschoben“ werden und dies irgendwann „auf den Betroffenen zurückfällt“. Im Grunde beruht eine gesamte „Datenwirtschaft“ auf solchen (Datenkauf-) Ketten. Dabei steht hier nicht so sehr der populäre Irrtum im Vordergrund, die freie Zugänglichkeit von Daten mache diese automatisch „vogelfrei“. Das Recht auf informationelle Selbstbestimmung und der Datenschutz gelten im Grundsatz auch dann noch, selbst wenn die Möglichkeiten, frei zugängliche Daten wieder „einzufangen“, stark begrenzt sein mögen. Aus diesem Grund ist zum Beispiel das Erheben von Daten aus Impressumsangaben oder aus dem Handelsregister zu Werbezwecken durchaus nicht unproblematisch, weil die Betroffenen hier rechtlich zu anderen Zwecken (Publizitätswirkungen des Handelsregisters, Transparenz über Verantwortlichkeiten beim Betreiben von Webseiten) gezwungen wurden, ihre Daten frei zugänglich zu machen, und dies nicht einfach zu anderen Zwecken ausgenutzt werden darf. Das mag bei Daten im „exhibitionistischen“ Social-Media-Umfeld im Einzelfall anders zu bewerten sein.
Das Problem liegt hier darin, dass Daten zwischen Verantwortlichen (im datenschutzrechtlichen Sinne) hin- und herübermittelt werden, ohne dass der Betroffene davon Kenntnis erlangt. Ob solche Übermittlungsvorgänge, insbesondere auch das „Kaufen von Daten“ bei entsprechenden Agenturen / Datenhändlern etc., eine Pflichtinformation auslösen müssen, ist nach wie vor eines der ungelösten Rätsel der DSGVO. Auf Empfängerseite könnte diese Pflichtinformation durch ein Erheben der Daten „nicht bei der betroffenen Person“ (Art. 14 DSGVO) ausgelöst werden, das im „Übermittelterhalten“ liegt. Ob dieses „Übermittelterhalten“ begrifflich eine „Dritterhebung“ ist, bleibt aber unklar. Auf Absenderseite kann die Pflichtinformation durch eine Zweckänderung ausgelöst werden, wenn die Daten ursprünglich nicht (transparent) auch zum Zweck der Übermittlung erhoben wurden. Ein Argument aus der Perspektive des – möglicherweise von einer unerwarteten Übermittlung überraschten – Betroffenen, das für eine (vorherige) Pflichtinformierung durch den Absender sprechen könnte, ist, dass die Zwecke, zu denen der Empfänger die Daten verarbeitet, möglicherweise abweichen von den Zwecken, zu denen der Absender die Daten verarbeitet hat, und die Übermittlung auch Auswirkungen auf die Ausübung von Betroffenenrechten haben kann. Die neuen Zwecke, nachdem sich die Daten nun (zusätzlich auch) in den Händen eines weiteren Verantwortlichen befinden, könnten für die betroffene Person „gefährlicher“ sein als die vormaligen Zwecke, und die Betroffenenrechte könnten gegenüber dem weiteren Verantwortlichen schwieriger auszuüben sein. Auf derartige Fragestellungen werden wir unten noch zurückkommen.

Auch hier kann man sich als Betroffener leicht ausmalen, wie viele Pflichthinweise man da eigentlich jeden Tag bekommen sollte, aber tatsächlich nicht bekommt. Nach einem populären Fall in Polen ist alleine der Umstand, dass eine solche Versendung von Hinweisen per Post erfolgen müsste und/ oder an sehr viele betroffene Personen verschickt werden müsste, kein „unverhältnismäßiger Aufwand", der ein Absehen von der Information rechtfertigen könnte.

Man kann diese beiden Ansätze auch zusammenführen, indem verschiedene Akteure ihre Daten über einen Betroffenen „zusammenlegen" (auch gegen Geld „zusammenkaufen") und daraus für einen oder mehrere Beteiligte neue Erkenntnisse über die Person gewinnen. Als gerichtliche Entscheidungen im Umfeld solcher Aktivitäten sind einerseits die Facebook-Custom-Audience-Entscheidung des Bayerischen Verwaltungsgerichtshofes and andererseits die Fashion-ID-Entscheidung des EuGH zu nennen. Beide Fälle handeln letztlich davon, dass Daten, die ein Akteur über einen Betroffenen „hat", mit den Daten eines anderen Akteurs zusammengeführt und die dadurch entstehenden Vorteile – von einem oder beiden – genutzt werden. Man kann derartige Konstellation noch dadurch abwandeln, dass die Zusammenführung von Daten durch einen oder mehrere Auftragsverarbeiter der beteiligten Verantwortlichen (auf deren Weisung hin) geschieht, und dass dies in einer (technischen) Weise geschieht, bei der kein Beteiligter die Ausgangsdaten der anderen Beteiligten „sieht", sondern nur das Ergebnis in Form einer gemeinsamen Erkenntnis über den Betroffenen. Eine solche Zusammenlegung von Datensammlungen kann, kartellrechtlich gesprochen, sowohl in Horizontalverhältnissen unter Wettbewerbern als auch in Vertikalverhältnissen zwischen verschiedenen Produktions- und Handelsstufen („Lieferkette") stattfinden. Ob solche Konstellationen datenschutzrechtlich zu einer Stellung als gemeinsam Verantwortliche führen (und damit eine Vereinbarung zwischen den Parteien notwendig machen), ist eher eine „technische" Folgefrage. Entscheidend ist auch hier zunächst, dass ein zusätzlicher Erkenntniswert und meist auch zusätzliche personenbezogene Daten generiert werden, also eine Erhebung stattfindet, die gegenüber dem Betroffenen transparent beschrieben werden muss, ggf. in Erweiterung des bisherigen Verarbeitungszwecks, die dem Betroffenen ebenfalls mitgeteilt werden muss.

Für die Verantwortlichen in derartigen Konstellationen stehen zwei Fragen im Vordergrund: Darf ich das? Und: Wann muss ich den Betroffenen worüber informieren? Beide Fragen bergen Sprengstoff und werfen für die Unternehmensführung häufig die Folgefrage auf, wie man sich als ordentlicher und gewissenhafter Unternehmensleiter bzw. Geschäftsführer in Situationen rechtlicher Unsicherheit verhalten soll. Aus rechtlicher Sicht ist das eine Frage der Organhaftung im Compliance-Kontext, aus Management-Sicht eine Frage des „risk appetite" bezüglich späterer Auseinandersetzungen einschließlich Schadensersatz- und Bußgeldfolgen sowie dem

möglicherweise eintretenden Rufverlust. Auf beides soll hier aber nicht näher eingegangen werden, und auch nicht auf die Frage, wie es sein kann, dass derart wichtige Fragen in einer Datenwirtschaft nicht durch den Gesetzestext klar beantwortet werden können.

Zweck und Granularität

Die wissenschaftlich-theoretische Diskussion über die DSGVO fokussiert sich seit längerem auf die sogenannte „Schutzgutdebatte", also welche abstrakten Rechtsgüter die DSGVO eigentlich genau schützt. Dabei liegen die praktischen Probleme ganz woanders, nämlich insbesondere im Bereich der Granularität. Das kann anhand der vorstehenden Fälle zunächst sehr gut in Bezug auf den Verarbeitungszweck illustriert werden.

Es ist ein großes Mysterium des EU-Rechts, warum es zu jeder Richtlinie und jeder Verordnung „Erwägungsgründe" gibt. Diese Erwägungsgründe sind meist, so auch bei der DSGVO, keine Erwägungsgründe im Sinne einer Herleitung, warum eine bestimmte Regelung erdacht wurde, sondern enthalten ihrerseits Regelungen. Ein gutes Beispiel ist der letzte Satz von Erwägungsgrund 47 der DSGVO: *„Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden". Man hätte diesen sprachlich etwas tapsigen Satz genauso gut – oder besser – in den Text der DSGVO-Artikel selbst schreiben können. Vorliegend soll es aber nicht um die (faktische) „Regelungswirkung" dieses Satzes gehen, sondern darum, ob die DSGVO damit etwas über die geforderte Granularität von (kommunikationsbedürftigen) Verarbeitungszwecken aussagen will. Personenbezogene Daten sollen ja „für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden" (Art. 5 DSGVO), und der Verantwortliche soll dem Betroffenen „die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen", mitteilen (Art. 13/14 DSGVO). Der Grundsatz der Zweckbindung ist ein hohes Gut innerhalb der DSGVO. Das sagt aber noch nichts darüber aus, wie eng oder weit ein „eindeutiger" Zweck sein darf. Wir lesen ergänzend – aber nicht erhellend – in Art. 22 Abs. 2 DSGVO: „Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht."*

Ist also pauschal „Direktwerbung" eine im datenschutzrechtlichen Rahmen zulässige Zweckdefinition? Stellt man sich auf diesen Standpunkt, kann man die oben heraufbeschwörte „Inflation" von Pflichtinformationen vielleicht vernachlässigen. Wenn Daten zum einheitlichen Zweck der „Direktwerbung" erhoben, übermittelt, angereichert

und zusammengeführt werden, dann stellen viele (Folge-) Aktivitäten keine Zweckänderung dar. Und dann ist möglicherweise auch die Notwendigkeit für einen Datenempfänger, der betroffenen Person die Selbstverständlichkeit mitzuteilen, dass auch er die empfangenen Daten zum Zwecke der Direktwerbung verarbeitet, im Rahmen der Auslegung der DSGVO hinsichtlich der Reichweite der Pflichtinformationen bei Übermittlungsvorgängen als gering einzuschätzen. Solange man also die Verarbeitung irgendwie mit Direktwerbung assoziieren kann, wäre alles über die in Erwägungsgrund 47 im Grunde vorweggenommene Interessenabwägung rechtfertigbar. Vorweggenommen wird die Interessenabwägung in diesem Erwägungsgrund deshalb, weil eine solche Abwägung sich – zumal im Massengeschäft – notwendigerweise (als eine Art „mutmaßliche Einwilligung") anhand abstrakt-typisierter Betroffeneninteressen vollziehen muss, und wenn die DSGVO-Macher der Meinung gewesen wären, dass sich das Betroffeneninteresse (an einer Vermeidung von Ärger, Aufwand, Beobachtetwerden und Hilflosigkeit durch Direktwerbung, s. o.) abstrakt und typischerweise über das Interesse des Verantwortlichen an Direktwerbung hinwegsetzen würde, hätten sie wohl den letzten Satz von Erwägungsgrund 47 nicht so geschrieben.

Nun kann man argumentieren, dass das Wort „Direktwerbung" in den zitierten Textstellen nur als „Oberbegriff für viele konkretere Zweckdefinitionen im Bereich Direktwerbung" gemeint ist. Selbst wenn man das nicht so sehen wollte, gibt es immer noch den klugen Satz, dass das Gesetz klüger ist als der Gesetzgeber, womit natürlich gemeint ist, dass die das Gesetz auslegenden Gerichte bisweilen klüger sein müssen als der Gesetzgeber, um das Gesetz „sinnvoll" anwenden zu können. Das wiederum ist eine Umschreibung dafür, dass der „gesunde Menschenverstand" eines Richters zielführender sein kann als der politische Menschenverstand der Politiker oder der bürokratische Menschenverstand der Exekutivbeamten, die den Gesetzestext geschrieben und verabschiedet haben. Diese Form von „overruling" kann auch in eine Auslegung gegen den Wortlaut – die aber meist dennoch als „korrigierende" Auslegung bezeichnet wird – ausarten. Das Amtsgerichts Pfaffenhofen hat die implizite Wertung des Erwägungsgrundes 47, dass „Direktwerbung" ein legitimer Zweck im Rahmen der Interessenabwägung ist, der das Betroffeneninteresse im Regelfall überwiegt (sonst hätte kein Grund bestanden, die Direktwerbung als legitimes Interesse eines Verantwortlichen hervorzuheben), in einer sehr durchgreifenden Weise „präzisiert". Es fragt, unter Einbeziehung der vernünftigen Erwartungshaltung des Betroffenen und der Branchenüblichkeit, nach einer „geschäftlichen oder persönlichen Beziehung" zwischen dem Verantwortlichen und dem Betroffenen, eine Einschränkung, die dem im Erwägungsgrund verwendeten Wort „Direktwerbung" nicht entnommen werden kann. Nach der Entscheidung – unterstellt, der EuGH hätte sie getroffen – würde also Erwägungsgrund 47 richtigerweise so zu lesen sein: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden, sofern eine

(geschäftliche oder persönliche) Beziehung zwischen dem Verantwortlichen und der betroffenen Person bestand“. Auf diesen wichtigen Aspekt ist seinerzeit bei der Abfassung der DSGVO aber offensichtlich niemand gekommen, sondern das musste von den Verantwortlichen (z. B. aus Kommentarliteratur) „erspürt“ werden, bevor ein Gericht diese (vermeintliche) Selbstverständlichkeit aussprach. Allein dies zeigt bereits Wohl und Wehe der gerichtlichen Auslegung der DSGVO. Nun wird aber jeder kluge Jurist gleichwohl einwenden, dass man das nicht so pauschal sagen könne, es komme vielmehr auf die Umstände des Einzelfalles an, z. B. auf die Branchennähe, d. h. wenn der Rechtsanwalt eine E-Mail mit Werbung für Gerichtsroben (oder auch nur Anzüge?) erhalten hätte, dann hätte man die Sache schon wieder ganz anders sehen können. Das ist die oben beschriebene Crux mit den Präzedenzfällen. Man hätte auch kaum glauben können, dass Gesetzesinterpretation einfach ist, wenn ganze Berufsstände ihre Existenz solchen Problemen verdanken.

Ebenso knifflig ist die Frage, was in einer Pflichtinformation an den Betroffenen hätte stehen müssen, wenn der spätere Versender der Werbe-Mail bei Erhebung (bzw. Einkauf) des maßgeblichen Datensatzes eine solche versendet hätte (was mutmaßlich schon vor der ersten Werbe-E-Mail zu einem Widerspruch, zu einem Auskunftsverlangen oder auch zu einer sofortigen Abmahnung wegen DSGVO-widriger Verarbeitung durch den Betroffenen geführt hätte). Das OLG Stuttgart hat in einem Urteil vom Mai 2021 ausgeführt, dass bei einer Verarbeitung personenbezogener Daten *„der Zweck (vorher) konkret (und formgerecht) festgelegt sein muss. Die Festlegung muss zu Beginn der Maßnahme erfolgen. Ansonsten würde die Anforderung ins Leere laufen, wenn stets im Nachgang der passende Zweck „konstruiert“ werden könnte. Erforderlich ist eine Dokumentation des Zwecks. Die Pflicht zur konkreten Festlegung dient der Überprüfung der Maßnahme durch den Verantwortlichen vor ihrer Durchführung und soll die Überprüfung durch die Datenschutzbehörden ermöglichen. Für den Zulässigkeitstatbestand der Wahrnehmung berechtigter Interessen spielt dies eine erhöhte Rolle, da sonst dem Recht auf informationelle Selbstbestimmung nicht ausreichend Rechnung getragen würde. Der konkrete Zweck der Datenverarbeitung ist hinreichend präzise zu benennen. Eine bloße Aufführung des Zwecks als „zur Gefahrenabwehr“ oder „zur Strafverfolgung“ genügt diesem Erfordernis nicht. Entsprechend der Formvorgabe nach Art. 30 Abs. 3 DSGVO muss der Zweck schriftlich oder elektronisch niedergelegt werden“*.

Ob nun „Direktwerbung“ ähnlich unpräzise ist wie aus Sicht des OLG Stuttgart „zur Gefahrenabwehr“ oder „zur Strafverfolgung“, bleibt offen – darüber hatte das OLG Stuttgart nicht zu entscheiden. In der juristischen Kommentarliteratur wird eine „Verwendung zur Werbung“ wohl als zu weit angesehen. Die Verwendung des unbestimmten Begriffs „Werbung“ wird nur dann für zulässig gehalten, wenn der Begriff

durch den Kontext seiner Verwendung hinreichend eingegrenzt ist (und damit „eigentlich“ nur eine stark begrenzte Art von Werbung umfassen soll). Umgekehrt soll aber der Grundsatz gelten, dass der Zweck umso konkreter gefasst werden muss, je stärker die „Belastung“ des Betroffenen ist, und es sind durchaus wesentlich stärkere Belastungen eines Betroffenen als durch unverlangte Werbung vorstellbar. Vielleicht hätte in den hypothetischen Pflichtinformationen im Fall des Amtsgerichts Pfaffenhofen als Zweckangabe stehen müssen: „Versendung von Werbe-Mails gegenüber unternehmerisch oder freiberuflich tätigen Personen, mit denen bislang keine Beziehung besteht, ohne Rücksicht darauf, in welcher Branche diese tätig sind“. Dann hätte der Verantwortliche vielleicht auch von vornherein mehr Zweifel entwickelt, ob es überhaupt zulässig ist, die Daten zu diesem, sehr konkret beschriebenen Zweck zu erheben bzw. zu erwerben und zu verarbeiten. Die Frage ist aber, ob ein Rechtsanwender überhaupt eine Sensibilität gehabt hätte, sich über diese Formulierung so tiefgehende Gedanken zu machen, und dass bei der Formulierung von Pflichtinformationen ein Heer von Datenschutzanwälten involviert ist, ist eher unwahrscheinlich.

Eine derart präzise Zweckdefinition wird in aller Regel dazu führen, dass der Zweck auch inhaltlich enger ausfällt. Dies führt zu einem Interessengegensatz, den die DSGVO (bewusst?) nicht auflöst und den die Kommentarliteratur so skizziert: *„Je konkreter die Zweckbestimmung ist, umso eher ergibt sich eine Zweckänderung, die einer neuen rechtlichen Rechtfertigung durch eine Einwilligung oder einen (anderen) Rechtfertigungsgrund bedarf. Der Verantwortliche wird daher oftmals ein Interesse daran haben, die Zweckbestimmung bei der Erhebung grundsätzlich vage zu halten, um somit erst spät in den Bereich der Zweckänderung zu geraten. Dem Betroffenen wiederum muss an einer konkreten Zweckbestimmung gelegen sein.“* Das klingt so, als würden Verantwortlicher und Betroffener über die Zweckbestimmung verhandeln, was, wie oben dargestellt, natürlich nicht der Fall ist. Aber man kann festhalten: Ein präziser bzw. enger Zweck ist zwar „datenschutzfreundlich“, würde aber bei inhaltlichen Operationen mit den Daten bedeuten, dass jedes Überschreiten dieses Zwecks – einschließlich Übermittlung und Empfang – sofort zu einer Zweckänderung führt. Entsprechend würde eine Vielzahl von Zweckkompatibilitätsprüfungen und Änderungs- bzw. Erhebungs-Pflichtinformationen notwendig. Will man hier als Unternehmen (vordergründig) Risiken einer zu unkonkreten Zweckdefinition vermeiden, müsste man „ins Blaue hinein“ vorab viele weitere, teils spekulative, enge bzw. präzise Zwecke auflisten, von denen aber der Verantwortliche noch nicht weiß, ob er sie überhaupt jemals benötigt, bzw. nach dem sprichwörtlichen „Murphy’s Law“ keiner so recht passt, wenn der Verantwortliche später „auf neue Ideen kommt“, was er mit den Daten noch gerne machen würde.

Man hätte in der DSGVO beispielhaft Zwecke aufführen können, um Klarheit über das „gewünschte“ Maß an Granularität für die Zweckdefinition zu vermitteln, was aber nicht

geschehen ist. Auch die Auffassungen der Behörden hierzu haben sich gewandelt. In Muster-Pflichtinformationen der Aufsichtsbehörden zu Beginn der DSGVO-Zeit (Mai 2018) wurden Zwecke eher „großzügig" umschrieben, mittlerweile werden derart definierte Zwecke in der Praxis als zu weit gerügt. Dabei ist nicht nur der Wortlaut der schriftlichen Definition in Pflichtinformationen maßgebend, sondern auch der Kontext. Wenn ein Arbeitgeber etwa „Arbeitsverhältnis" als Zweck angeben würde, wäre das – anhand der Umstände ersichtlich und damit grundsätzlich auslegungsfähig – nur eine Verkürzung dessen, was in Art. 88 DSGVO ausführlich beschrieben wird mit *„für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisse"*.

Direktwerbung als Zweck

Vermutlich werden statistisch die meisten Daten (zumindest vorgeblich) zu Direktwerbungszwecken im weiteren Sinne erhoben. Daher lohnt, aufbauend auf der oben beispielhaft dargestellten Zweckformulierung, eine genauere Beschäftigung mit möglichen Zweckdefinitionen in diesem Bereich vor dem Hintergrund weiterer Backend-Verarbeitungshandlungen. Dabei geht es nur um die formale Zweckdefinition und die Zweckbindung als solche, nicht um die Frage, ob der Zweck (im Sinne einer datenschutzrechtlichen Legitimationsgrundlage) gerechtfertigt werden kann. Will ein Unternehmen Adressdaten von einem Adresshändler kaufen, mit Brancheninformationen und eigenen Erkenntnissen zusammenführen, mit einem „befreundeten Unternehmen" abgleichen (das möglicherweise noch weitergehende Informationen zu denselben Personen hat), die Form und den Inhalt einer Werbemaßnahme per KI „maßgeschneidert" für die Person definieren und das Ergebnis wiederum auch anderen „Käufern" zur Verfügung stellen, kann man diese Verarbeitung so beschreiben:

„Direktwerbung".

Man kann es aber auch so beschreiben:

„Verwendung zu Zwecken der Direktwerbung im Sinne (a) der Zusammenführung mit frei zugänglichen Brancheninformationen und weiteren dem Verantwortlichen vorliegenden Daten, (b) der Zusammenführung mit gleichartigen Daten anderer Marktteilnehmer, (c) der Anwendung und des Training von Algorithmen, die anhand der Daten Form und Inhalt

von Direktwerbemaßnahmen bestimmen und (d) der Übermittlung an andere Marktteilnehmer zu denselben Zwecken".

Der Vorteil dieser zweiten Formulierung ist, dass hier bereits einige „Backend-Nebenzwecke" ausdrücklich mit eingeführt wurden, sodass deren spätere Umsetzung keine Zweckänderung mehr darstellt. Demgegenüber wird man bei der Verwendung eines Ein-Wort-Zweckes immer interpretieren müssen, was sich der Betroffene als Adressat der datenschutzrechtlichen Pflichtinformation darunter vorstellen musste – die klassische Auslegung vom „objektivierten Empfängerhorizont" her. Mit dieser Interpretation eines Ein-Wort-Zweckes geht natürlich eine erhebliche Rechtsunsicherheit für den Verantwortlichen einher, insbesondere deshalb, weil ein Betroffener solche Backend-Nebenzwecke nicht „riechen" kann. Ein Gericht würde daher häufig dazu tendieren, dass Backend-Nebenzwecke kein Teil des Ein-Wort-Zweckes waren, und bei einer Verarbeitung zu diesen weiteren Zwecken eine Zweckänderung annehmen. Dies gilt umso mehr, je weniger ein Betroffener anhand der Umstände – eine kurze Werbeeinwilligung, eine punktuelle Geschäftsbeziehung zum Verantwortlichen, eine Erhebung der Daten nicht beim Betroffenen selbst, eine einfache Interessenabwägung – von solchen Nebenzwecken ausgehen musste, sondern einen geradlinigen, aufrichtigen, überschaubaren Zweck unterstellen durfte. Vielleicht wird man sogar anhand der grundsätzlichen Beweislastverteilung, wonach der Verantwortliche die Zulässigkeit der Datenverarbeitung und nicht die Aufsichtsbehörde oder der Betroffene deren Unzulässigkeit derselben nachzuweisen hat, davon ausgehen müssen, dass in Zweifelsfällen nur der „kleinstmögliche Begriffskern" als tatsächlich angegebener Zweck gelten kann. Im AGB-Recht (Verbraucherschutz!) würde dies dem Grundsatz der sog. „verwenderfeindlichsten" Auslegung von AGB-Klauseln entsprechen.

Der Nachteil der zweiten Formulierung liegt darin, dass das Risiko einer „Beanstandung" durch den Betroffenen (mit entsprechender Verweigerung einer Einwilligung bzw. Widerspruch gegen die Verarbeitung) wesentlich höher ist, wenn er im Rahmen der Pflichtinformationen von solchen „Backend-Nebenzwecken" erfährt. Außerdem werden diese Nebenzwecke über die Pflichtinformationen auch für Dritte – Datenschutzbehörden, Presse, Ermittlungsbehörden etc. – publik und können auch ohne Betroffenenbeschwerde zu entsprechenden Nachforschungen führen. Und für den einen oder anderen Mitarbeiter beim Verantwortlichen – einschließlich des betrieblichen Datenschutzbeauftragten – kann der Zwang zur „nicht mehr nur nebulösen" Formulierung von Zweckdefinitionen dazu führen, dass die Berechtigung zur Verarbeitung zu den Nebenzwecken hinterfragt wird. Das kann beispielsweise in der Erkenntnis münden, dass außerhalb des Begriffskerns „Direktwerbung" (d. h. dem Speichern und Verwenden selbst erhobener Kunden- und „Target"-Kontakte) aufgrund der Form der Backend-Verarbeitung, „insbesondere bei Verwendung neuer Technologien", eine Datenschutz-

Folgenabschätzung notwendig ist. Welcher Verantwortliche würde da nicht lieber beim schlichten Ein-Wort-Zweck bleiben und das Restrisiko einer zu unkonkreten Zweckdefinition akzeptieren (Stichwort „risk appetite“, siehe oben)? „Let sleeping dogs lie“ heißt es dazu im Englischen noch treffender als in der deutschen Fassung („wecken“). Die Konsequenz eines im Verhältnis zur tatsächlichen späteren Verarbeitung zu eng definierten Zwecks – entweder, weil sich aus dem Empfängerhorizont ein weiterer Zweck nicht ergeben musste, oder weil der Zweck tatsächlich sehr eng formuliert war – dürfte sein, dass die Daten unabhängig von der Frage der Legitimationsgrundlage für einen anderen Zweck nicht verarbeitet werden dürfen. Denn Daten, die auf Basis einer (nicht nur in Petitessen) ungenügenden Pflichtinformation erhoben wurden, die auch nicht durch eine Zweckänderungsmitteilung nachträglich erweitert wurden, sind unter Verstoß gegen das Datenschutzrecht erhoben worden und damit „toxisch“, d. h. ihre Weiterverarbeitung ist datenschutzrechtlich nicht zu rechtfertigen. Mit anderen Worten: Die gesamte weitere Verwertungskette wankt. Dies betrifft auch Empfänger der unrechtmäßig erhobenen Daten, denen die Daten übermittelt oder anderweitig zur Verfügung gestellt werden. Es tut daher jeder Empfänger (einschließlich Käufer) von Daten gut daran, die Herkunft der überlassenen Daten hinreichend genau zu untersuchen, also mit welchen Zweckdefinitionen, Pflichtinformationen und Legitimationsgrundlagen die Daten erhoben wurden (sowie wie beweisbar die Einhaltung des Datenschutzrechts durch den „Datenvorgänger“ jeweils ist), und sich die Einhaltung des Datenschutzrechts vom Übermittelnden versichern zu lassen. Ab welchem Grad von „Due Diligence“ der Empfänger tatsächlich nachweisen kann, dass er, wenn doch in den vorherigen Kettengliedern etwas schiefgegangen sein sollte, „in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist“ (Art. 82 Abs. 3 DSGVO), ist nach wie vor ungeklärt.

Daten, Daten, ihr müsst wandern

Es war oben bereits die Rede davon, dass sowohl Zweckänderungen als auch ggf. der Empfang personenbezogener Daten – als Erheben im Sinne von Art. 14 DSGVO – informationspflichtig sind. Im Kontext der Erhebung formuliert die DSGVO, dass der Verantwortliche der betroffenen Person etwas „mitzuteilen“ hat (Art. 13 Abs. 1, 14 Abs. 1 DSGVO). Bei Zweckänderungsmitteilungen spricht die DSGVO davon, dass dem Betroffenen Informationen „zur Verfügung zu stellen“ hat. Ob das ein Unterschied ist, wird aus dem Text der DSGVO nicht klar, auch wenn zumeist behauptet wird, es sei dasselbe mit unterschiedlichen Worten gemeint worden.

Werden Daten vom Verantwortlichen A an den Verantwortlichen B weitergegeben, möchten natürlich beide Verantwortliche – insbesondere dann, wenn sie sich „nur“ auf ein berechtigtes Interesse stützen – diese Datenübermittlung nicht (jedes Mal) extra publik

machen. Ausnahmevorschriften, nach denen auf eine Information des Betroffenen verzichtet werden kann, soweit er die Informationen schon kennt, machen eine Benachrichtigung insgesamt nur dann obsolet, wenn der Betroffene sämtliche Informationen schon kennt. Die im Moment einer Informationsübermittlung bereits bestehende Kenntnis des Betroffenen von Sender, Empfänger, Zweck, Speicherdauer, weiteren Empfängern etc. ist aber eher die unwahrscheinlichere Variante. Der Verantwortliche A wird also versuchen, sämtliche möglichen Datenweitergaben bereits im Rahmen der ursprünglichen Erhebung vom Betroffenen als Zwecke zu definieren, um sich eine spätere Zweckänderung zu ersparen. Der Verantwortliche B wird versuchen, sich vom Betroffenen den Empfang von Daten vom Verantwortlichen A vorab „freizeichnen" zu lassen. So wird in den „Schufa-Klauseln", die z. B. von Banken gegenüber Betroffenen verwendet werden, die Weitergabe von Informationen an die Schufa legitimiert und auch gleichzeitig die Pflichtinformationen der Schufa beigefügt. Diese Pflichtinformationen legitimieren wiederum die Weitergabe durch die Schufa an Dritte, die Bonitätsauskünfte anfragen, und die Zwecke werden neben der Kreditwürdigkeitsbeurteilung erweitert um „Betrugsprävention, Seriositätsprüfung, Geldwäscheprävention, Identitäts- und Altersprüfung, Anschriftenermittlung, Kundenbetreuung oder Risikosteuerung sowie Tarifierung oder Konditionierung".

Auf Empfängerseite – also im Beispiel aufseiten des (weiteren) Verantwortlichen, der eine Schufa-Auskunft über einen Betroffenen abfragt – ist die Situation nur dann einfach zu handhaben, wenn der Empfänger vorher bereits einen „direkten Draht" zum Betroffenen hat. Dann kann er den Betroffenen etwa bei Aufnahme einer Vertragsbeziehung darüber informieren, welche Daten er aus welchen Quellen hinzuzuziehen gedenkt, und kann dies in seine Pflichtinformationen integrieren. Ansonsten droht die Pflicht, den Betroffenen, wenn der Verantwortliche Daten „nicht bei der betroffenen Person erhebt" (Art. 14 DSGVO), über den Empfang gesondert zu benachrichtigen, soweit er über eine Kontaktmöglichkeit verfügt.

Zwei Beispiele sollen das verdeutlichen. Ein Unternehmen plant gemeinsam mit einer Unternehmensberatung ein Umstrukturierungsprojekt und ermittelt in diesem Rahmen Mitarbeiter, die befördert oder versetzt (oder abgebaut) werden sollen. Im Zuge des Projekts ergibt sich, dass immer neue Details über die zu bewertenden Mitarbeiter notwendig sind, und in einem späteren Stadium führt die Unternehmensberatung auch selbst Interviews mit den Betroffenen. Hierbei wird die Unternehmensberatung begrifflich kein Auftragsverarbeiter sein, sondern ein eigenständiger Verantwortlicher, weil der Gegenstand der Beauftragung nicht die Verarbeitung von Daten, sondern die Erbringung höherwertiger Beratungs-Dienstleistungen ist. Die Unternehmensberatung erhebt die Daten „kunterbunt" teils bei den Betroffenen, teils nicht bei den Betroffenen, und steht selbst in keinem (Vertrags-) Verhältnis zu den Betroffenen selbst. Für Daten, die sie vom

Arbeitgeber erhält, müsste sie dem Betroffenen, über dessen Kontaktdaten sie wohl verfügen wird, Pflichthinweise zukommen lassen, wenn man davon ausgeht, dass der „Übermittlungsempfang“ eine Erhebung darstellt. Davon könnte sie der Arbeitgeber auch nicht „befreien“. Diese Pflichthinweise würden das Projekt natürlich intern publik machen, wenn bisher „im Verborgenen“ gearbeitet wird, weshalb die Motivation nicht groß sein wird, hier in großem Umfang entsprechende Informationen abzusetzen. Oder: Ein Unternehmen kauft Datensätze von einem Anbieter von Branchen- bzw. Firmeninformationen, um an Namen und Adressen von Beirats- und Aufsichtsratsmitgliedern mittelgroßer Unternehmen zu gelangen. Monate später wird ein „ausgesiebter“ Teil davon angeschrieben – zu welchem Zweck auch immer –, aber die Erlangung der Informationen müsste jeder betroffenen Person angezeigt werden, auch derjenigen, die am Ende nicht kontaktiert wird.

Plattformlogiken als Datensauger

Bisher ging es um die Perspektive verantwortlicher Unternehmen. Es gibt aber viele Bereiche, in denen die eigentliche (inhaltliche) Verarbeitung von Daten bei Auftragsverarbeitern stattfindet und nicht bei Verantwortlichen, und in denen – anders, als das Wort Auftragsverarbeitung es nahelegt – die Logik der Verarbeitungshandlungen das Geschäftsmodell des Auftragsverarbeiters darstellt. Traditionell stellt man sich einen Auftragsverarbeiter als „Rechenknecht“ oder „verlängerte Werkbank“ vor, insbesondere einen Rechenzentrumsbetreiber, der einfach nur Verarbeitungskapazität bereitstellt, auf der dann Software läuft, die der Verantwortliche selbst geschrieben oder zugekauft hat, auf jeden Fall aber selbst inhaltlich „betreibt“. Vordergründig ist dies das Geschäftsmodell der großen Cloud-Betreiber, die vorrangig skalierbare Rechenkapazität anbieten, ihre Dienste aber zugleich zunehmend durch das Angebot inhaltlicher Datenoperationen (etwa im KI-/Statistik-Bereich) erweitern.

Das Modell des Rechenzentrumsbetreibers, der gewartete Hardware- und Betriebssystem-Plattformen und Infrastrukturleistungen zur Verfügung stellt, wird zunehmend durch „Software as a Service“-Angebote ergänzt und teils ersetzt. Ging es früher darum, eine Software zu „kaufen“ und auf einer eigenen oder (an einen Rechenzentrumsbetreiber) outgesourcten IT-Landschaft zu betreiben, wird die Software mittlerweile als Plattform virtualisiert zur Verfügung gestellt. Dabei stehen natürlich zunächst einmal die Qualität und Effizienz im Vordergrund: Updates der Software können schneller installiert werden und stehen sämtlichen Kunden „sofort“ zur Verfügung, die zugrundeliegende Systemlandschaft des Anbieters ist überschaubarer als ein Flickenteppich von Systemlandschaften bei verschiedenen Kunden und sofort. Aber es kommt auch hinzu, dass die Daten der Kunden, also die „Nutzdaten“, dann beim Anbieter liegen und nicht beim Kunden bleiben. So kann ein Unternehmen, das früher „nur“ Softwarelogik

bereitgestellt hat, zum Plattformbetreiber werden und sich natürlich auch unentbehrlich machen. Die Migration von Daten von einer Plattform auf eine andere ist meist viel schwieriger als von einer Software in eine andere, wenn beide Software-Produkte „on premise“ eingesetzt werden. Kartellrechtlich würde man von einem (starken) „locked in“-Effekt sprechen.

Datenschutzrechtlich betrachtet wird der Verantwortliche so zum Datenlieferant, der mit diesen Daten „etwas machen lässt“ von jemandem, der davon mehr versteht. Die inhaltliche Logik stammt vom Plattformbetreiber, der die Dienste dieser Logik – datenschutzrechtlich im Gewand einer Auftragsverarbeitung – anbietet. Zwar mag der Zweck der Verarbeitung immer noch vom Verantwortlichen selbst gesetzt werden (je nachdem, wie man „Zweck“ definiert – s. o.), aber die Mittel und auch das Vorgehen im Einzelnen stehen unter der Herrschaft des Plattformbetreibers. Überhaupt kennzeichnet das Wort Plattformbetreiber die „Machtverhältnisse“ besser als „Dienstleister“ bzw. „Auftragsverarbeiter“: Der Verantwortliche muss den Dienst häufig so in Anspruch nehmen, wie es ihn gibt (inklusive der „Anlieferung“ seiner Daten) – oder es lassen.

Solche „Plattformbetreiber“ aggregieren ungeachtet ihrer datenschutzrechtlich „dienenden“ und strikt weisungsabhängigen Funktion erhebliche Datenmengen von verschiedenen Auftraggebern (Verantwortlichen). Trennung von Datenbeständen einzelner Kunden hin oder her: Mit der Datenmenge wachsen die Begehrlichkeiten, was die „Ausbeutung“ großer Datenbestände angeht. Da geht es den großen „Cloud-Riesen“ nicht anders als einem Start-up, das beispielsweise Unternehmen eine Lernplattform für deren Mitarbeiter anbietet. Der Datenbestand als Ganzes bietet Erkenntnismöglichkeiten, die nur die Daten eines Kunden nicht bieten würden. Die Begehrlichkeiten beginnen mit statistischen Übungen, also wie häufig der Dienst von wem genutzt wird. Das kann notfalls auch noch als für die Abrechnung gegenüber dem Kunden wichtig rechtfertigt werden. Weiter können mehr oder weniger ausgefeilte KI-Algorithmen eingesetzt werden, um statistische Größen zu ermitteln, etwa, wie produktiv die Mitarbeiter der verschiedenen Kunden sind. Natürlich benötigen die Algorithmen Daten, anhand derer sie weiterentwickelt werden können, was den Bedarf nach Echtdaten in großer Menge auslöst. Hierüber gibt es in der Fachwelt vielfältige Diskussionen, auch zur neuen EU-Regulierung von KI-Anbietern. Personalisiert könnten Erkenntnisse über einzelne Betroffene dem Kunden angeboten werden, der sich noch gar nicht damit beschäftigt hat, dass man solche Erkenntnisse aus „seinen“ Daten ziehen kann. Aber natürlich können neben dem Plattformbetreiber und dessen Auftraggebern auch Dritte an den Daten interessiert sein. Eine Marketing-Agentur möchte gerne wissen, in welchen Städten in Deutschland Mitarbeiter wann und wie produktiv oder lernfähig sind, um die Werbung für bestimmte Produkte entsprechend daran zu orientieren. Der Dienstleister kann aber auch – ohne oder mit Wissen des Kunden – anhand des Lernfortschritts

(personenbezogene) Profile der Mitarbeiter der Kunden erstellen und Dritten zum Kauf anbieten. Wäre es nicht am Personalvermittlungsmarkt eine nützliche Information, wenn die Mitarbeiter eines bestimmten Unternehmens im Schnitt eine niedrigere Produktivität aufweisen als die Mitarbeiter eines Konkurrenten? Natürlich kann das alles nicht nur Beschäftigtendaten, sondern auch Kundendaten eines Unternehmens betreffen oder die Daten anderer Betroffenengruppen, mit denen ein Unternehmen gehäuft zu tun hat und die es deshalb im Rahmen einer (erkenntnisversprechenden) Plattform verarbeiten lassen will.

Was nach einem einfachen „Auswringen" der zur Verfügung stehenden Daten klingt, wirft in der Praxis natürlich viele Probleme auf. Soweit dem Auftraggeber weitergehende Erkenntnisse über „seine" Mitarbeiter zur Verfügung gestellt werden, stellt sich die Frage, ob dies noch „zu Zwecken der Durchführung des Beschäftigungsverhältnisses" (§ 26 BDSG) erfolgen darf. Vor dem Hintergrund der in der Öffnungsklausel des Art. 88 DSGVO beschriebenen Zwecke, welche der nationale Gesetzgeber überhaupt im Beschäftigtendatenschutz genauer regeln darf, dürfte nicht verwundern, dass man dies mit guten Gründen verneinen kann. Hier gibt es zudem Themen wie Mitarbeiterüberwachung und Einbindung des Betriebsrats, die aufseiten des Kunden (also des Verantwortlichen) erwogen werden müssen. Soweit der Auftragsverarbeiter (Plattformbetreiber) die Daten offen oder heimlich zu eigenen Zwecken „abzieht" und auswertet, hängt die rechtliche Bewertung davon ab, ob die Daten in anonymer Form zweckentfremdet werden oder nicht. Bei der Anonymisierung ist immer noch rechtlich unklar, ob dies eine „Verarbeitungshandlung" im Sinne der DSGVO darstellt und demzufolge eine datenschutzrechtliche Legitimationsgrundlage erfordert. Besonders in der juristischen Literatur wird diese Frage häufig mit dem Argument bejaht, dass die DSGVO jedweden Umgang mit personenbezogenen Daten regeln wolle. Die Anonymisierung sei deshalb zumindest als unbenanntes Beispiel vom Verarbeitungsbegriff der DSGVO umfasst. Anders hat hingegen das LG Frankfurt in einem Urteil vom Januar 2017 zur damals geltenden Rechtslage (BDSG a.F.) entschieden. Ein Kfz-Sachverständigenbüro als Auftragsverarbeiter für Kfz-Versicherer hatte u. a. offensiv damit geworben, dass es „über eine Vergleichsdatenbank mit über 3 Millionen Schadensfällen pro Jahr verfüge", d. h. (ggf. neben anderen Datenquellen) über anonymisierte Auswertungen von im Auftrag begutachteten, personenbezogenen Schadenssachverhalten. Hiergegen ging ein Unfallteilnehmer vor, der seine Daten nicht für diesen Zweck verwendet wissen wollte. Das LG Frankfurt entschied, dass die Verwendung von personenbezogenen Daten zur Erstellung einer anonymisierten Auswertung sowie deren Speicherung und Verarbeitung datenschutzrechtlich unbedenklich sei, da anonymisierte Daten und damit auch deren „Herstellung" nicht dem Anwendungsbereich des BDSG a.F. unterfallen würden. Die datenschutzrechtliche Bewertung wurde vom OLG Frankfurt in der dazugehörigen Berufungsentscheidung im Februar 2019 bestätigt. Der Entscheidung des OLG lässt sich

am Rande entnehmen, dass die Verwendung personenbezogener Daten zur Erstellung anonymer Auswertungen auch unter der zwischenzeitlichen Geltung der DSGVO nicht zu beanstanden sein würde (auch wenn konkret nicht über einen Sachverhalt zu entscheiden war, der sich zum Zeitpunkt der Geltung der DSGVO zugetragen hatte). Folgt man der Rechtsprechung dieser Gerichte – neuere Entscheidungen zu diesem Thema liegen nicht vor –, so kann der Auftragsverarbeiter sämtliche Daten aller Kunden anonymisieren und (also nicht-personenbezogene Daten) verwerten, sei es als KI-Trainingsmaterial, als Basis für statistische Aussagen oder als „big data"-Datengrab für die Zukunft.

Werden die Daten in personenbeziehbarerer Form zu eigenen Zwecken des Plattformbetreibers verwendet, handelt es sich um einen sogenannten „Auftragsverarbeiter-Exzess" (Art. 28 Abs. 10 DSGVO). Dies ist für den Auftragsverarbeiter doppelt gefährlich und haftungsträchtig: Einerseits verstößt er gegen die Weisungsgebundenheit gegenüber dem Auftraggeber und verletzt seine Pflichten als Auftragsverarbeiter, andererseits wird er selbst zum Verantwortlichen, der die betroffenen Personen nicht richtig informiert hat und ihre Daten vermutlich ohne ausreichende datenschutzrechtliche Legitimationsgrundlage nutzt. Findet sich in den Vertragsbedingungen des Plattformbetreibers gegenüber den Verantwortlichen eine Regelung, wonach dem Plattformbetreiber diese „Zweckentfremdung" (im Verhältnis zum Verantwortlichen) erlaubt ist, kann das einerseits dem Rechtsverhältnis die Qualität als Auftragsverarbeitungsvereinbarung nehmen und andererseits eine datenschutzrechtliche nicht legitimierbare Datenweitergabe durch den Verantwortlichen darstellen.

Es gibt viele Plattformbetreiber, die sich aufgrund dieses Dilemmas dazu entschieden haben, selbst Verantwortlicher zu sein und kein Auftragsverarbeiter, eben weil sie die Daten ausdrücklich (und vor allem) für sich nutzen wollen. Dazu zählen etwa Social-Media-Plattformen wie Facebook. Statt eines Dreiecksverhältnisses zwischen der betroffenen Person, dem Verantwortlichen und dessen Auftragsverarbeiter oder zwischen der betroffenen Person und zwei unabhängigen Verantwortlichen in einer „Datenkette" ist dann – so hat es der EuGH entschieden – ein Dreiecksverhältnis zwischen der betroffenen Person und zwei gemeinsam Verantwortlichen anzunehmen. Im Beispiel oben würde die „Sogwirkung" des Arbeitgebers und der zumindest teilweise gemeinsam definierte Verarbeitungszweck dazu führen, dass die Daten dann von beiden Verantwortlichen – dem Arbeitgeber und dem Plattformbetreiber – gemeinsam verarbeitet werden. Jeder Verantwortliche müsste dann, abseits des überlappenden Zweckes, der gemeinsamen Verantwortlichenstellung und einer Vereinbarung nach Art. 26 DSGVO, einen eigenen (weitergehenden) Zweck definieren, die betroffene Person darüber (zusätzlich) informieren und eine eigene datenschutzrechtliche Legitimationsgrundlage „bereithalten". Im Rahmen des überlappenden Zwecks haftet dann auch der eine

Verantwortliche für das, was der andere Verantwortliche mit den Daten anstellt. In derartigen Konstellationen kann es dem Plattformbetreiber leichter fallen als dem anderen Verantwortlichen, eine wirksame Einwilligungserklärung von der betroffenen Person zur Erhebung von Daten mit weiter Zweckdefinition zu erhalten. Wer will nicht gerne „dabei sein"? Allerdings mehren sich europaweit die Bußgeldverfahren (und Bescheide) wegen zu unverständlicher und „maßloser" Einwilligungserklärungen mit vagen Zweckdefinitionen gegen große Plattformbetreiber – eine, wie eingangs dargelegt, paternalistische Rettung des hilflosen Betroffenen vor dessen gleichgültiger Überforderung mit derartigen Einwilligungserklärungen.

Wie oben gezeigt, muss der „Endzweck" solcher Informationsaggregation nicht immer personalisierte Werbung gegenüber dem Betroffenen sein. Facebook könnte durchaus Arbeitgebern, die ihre Arbeitnehmer auf Facebook „locken" bzw. dort mit ihnen vernetzt sind, anbieten, diese Arbeitnehmer bei ihren sonstigen Social-Media-Aktivitäten zu überwachen und dem Arbeitgeber „Auffälligkeiten" zu melden. Als Plattformbetreiber verfügt Facebook über den entsprechenden Datenpool und die entsprechenden Datensynergien bei der Auswertbarkeit und kann dem Arbeitgeber damit Erkenntnisse versprechen, die über den „Datenhorizont" des Arbeitgebers hinausgehen. Die Frage wäre hier eher, ob der Arbeitgeber diese Daten „annehmen" und selbst (weiter-) verarbeiten dürfte.

Im Bereich der Datenaggregation gibt es also Plattformen, die nach außen auftreten, und solche, die Daten über Betroffene nur „im Backend" erhalten. Tritt eine Plattform nach außen auf, ist es wahrscheinlicher, dass sie Daten über dieselben Betroffenen – die Plattform-Nutzer – aus verschiedenen Richtungen enthält. Das führt dazu, dass die mit einem „Kooperationspartner", etwa dem Facebook-Fanpage-Betreiber, gemeinsam verantworteten Daten nur einen kleinen Ausschnitt der Gesamtmenge an Daten über den jeweiligen Betroffenen ausmachen, die dem Plattformbetreiber vorliegen. Die Datensynergieeffekte beim Plattformbetreiber gehen also hier in die „Tiefe" des einzelnen Betroffenen: Während der Co-Verantwortliche bzw. auftraggebende Verantwortliche die betroffene Person vorrangig aus „seiner" Perspektive kennt, kennt der Plattformbetreiber die betroffene Person aus allen Perspektiven sämtlicher relevanter Verantwortlicher, und zusätzlich die Daten, die er direkt beim Betroffenen erhoben hat. Bei Plattformen hingegen, die im Innenverhältnis als Auftragsverarbeiter für verschiedene Verantwortliche tätig werden, ist es wahrscheinlicher, dass die Betroffenendaten, die von den einzelnen Kunden angeliefert werden (von den Betroffenen selbst werden sie dann nicht erhoben), keine bzw. keine erheblichen Schnittmengen aufweisen. Die Datensynergieeffekte ergeben sich dann hier vorrangig aus der „Breite" der Daten, d. h. man hat Daten zu denselben Datenkategorien (meist in Form strukturierter Datensätze) über viele Betroffene. Allerdings gibt es auch in diesem Bereich Plattformbetreiber, die gezielt nach „Matches"

suchen, also dass mehrere Auftraggeber Daten zum selben Betroffenen „einreichen“, die dann miteinander abgeglichen und Auffälligkeiten festgestellt werden können.

Dass die Datenschutzaufsichtsbehörden die Datenansammlungen in der Hand von „Plattformbetreibern“ nicht nur im Bereich sozialer Medien durchaus kritisch sehen, zeigt sich exemplarisch im Bereich der Lernplattformen im schulischen Bereich, die von externen (privatwirtschaftlichen) Dienstleistern betrieben werden. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit führt in ihren Hinweisen zum datenschutzkonformen Einsatz von digitalen Lernplattformen in Schulen vom April 2020 aus: *„Eine Nutzung der Daten zu eigenen Zwecken des Dienstleisters, beispielsweise zu Forschungszwecken, ist vertraglich auszuschließen oder lediglich aufgrund einer separaten Einwilligung der Erziehungsberechtigten bzw. Schülerinnen und Schüler zu ermöglichen. Eine Ablehnung der Einwilligung darf keine Einschränkung des Dienstes zur Folge haben.“ Dies ist Ausfluss einer Risikoeinschätzung aus der Betroffenenperspektive – die „Risiken für die Rechte und Freiheiten natürlicher Personen“ sind ja Dreh- und Angelpunkt der DSGVO –, wie die folgenden Ausführungen in der genannten Publikation zeigen: „Man muss sich klarmachen, dass der Einsatz von digitalen Lernplattformen nicht zu unterschätzende Gefahren für die Persönlichkeitsrechte sowohl von Schülerinnen und Schülern als auch von Lehrkräften mit sich bringen kann. So setzt die Nutzung entsprechender Plattformen in der Regel eine personalisierte Anmeldung voraus. Teilweise werden Daten erhoben, die für die Nutzung der Plattform gar nicht benötigt werden. Anbieter der Plattformen können häufig das Nutzungsverhalten der angemeldeten Schülerinnen und Schüler sehr genau auswerten. Als Folge können Persönlichkeitsprofile über die Schülerinnen und Schüler, aber unter Umständen auch der Lehrkräfte, entstehen, die von den Anbietern für wirtschaftliche Zwecke, wie zum Beispiel Werbung, genutzt werden können.“* Ähnliche Argumente werden auch im Kontext von Beschäftigtendaten erwogen werden müssen.

Was ist wichtig?

Der erste und wichtigste Schritt im Datenschutz heißt: Awareness. Jeder, der bei Verantwortlichen mit personenbezogenen Daten umgeht, diese entgegennimmt, be- und verarbeitet und weiterleitet – und vor allem: jeder, der Systeme konzipiert und programmiert, die dies automatisiert erledigen –, muss ein Bewusstsein dafür haben, dass diese Vorgänge rechtlich relevant sind. Die Erkenntnis, es mit einem rechtserheblichen Vorgang zu tun zu haben, ist die „halbe Miete“, denn oft besteht keine Sensibilität für diese Problemstellungen. Jedes Kind bekommt (hoffentlich) mitgegeben, was „Mord“ ist, aber was ein Datenschutzverstoß ist – und das gilt auch für andere Compliance-Rechtsgebiete –, ist kein Gegenstand „erlernter Sensibilität“.

Der zweite Schritt ist es, Datenflüsse, Beteiligte, Zwecke und Betroffene möglichst exakt zu definieren. Dies stellt viele Verantwortliche vor große Probleme. Das Management und, sofern es sie gibt, die Compliance-Abteilung oder der Datenschutzbeauftragte wissen häufig gar nicht, welche Daten von welchen Betroffenengruppen überhaupt irgendwo verarbeitet werden. Man kann aber nur dann beurteilen, welche Risiken es gibt und was zur Risikominimierung getan werden muss, wenn man überhaupt weiß, dass es ein Risiko gibt. Die Trennung im Unternehmen in Faktenkenntnis (auf Abteilungsebene) und Rechts- bzw. Risikobewertungsfähigkeit (auf Ebene von Management, Compliance-Abteilung und Datenschutzbeauftragtem) führt zu einem negativen Kompetenzkonflikt: Niemand fühlt sich zuständig. Werden mögliche Datenschutzverstöße in der Öffentlichkeit, bei den Betroffenen oder bei den Aufsichtsbehörden publik, schützt Unwissenheit vor Strafe nicht, auch wenn es nach wie vor eine ungelöste – zwischen erstinstanzlichen Gerichten umstrittene – Frage ist, ob Bußgelder gegen Unternehmen nur verhängt werden dürfen, wenn den Leistungsorganen (Geschäftsführung / Vorstand) ein persönliches Fehlverhalten (einschließlich eines Unterlassens) vorgeworfen werden kann.

Man kann nun die Frage stellen, warum die Zahl der (öffentlich bekannten) Verfahren in Bezug auf die Backend-Verarbeitung personenbezogener Daten so niedrig – im Vergleich zum „Frontend“ gegenüber dem Betroffenen – ist, wenn es in diesem Bereich so viele unentdeckte Probleme gibt. Die Antwort darauf ist ganz einfach: Die Kontrolldichte ist bislang ausgesprochen niedrig und die Betroffenen erfahren von vielen Operationen mit ihren Daten nichts. Nicht einmal Auskunftsersuchen nach der DSGVO werden zwangsläufig die Komplexität der Datenflüsse offenlegen, sondern nur die Daten selbst und ggf. ein kleines „Spotlight“ auf Herkunft und/oder Empfänger von Daten, oft nur der Kategorie nach beschrieben. Es hat bislang kaum jemand versucht, den Weg seiner Daten (und deren Kopien) durch die verschiedenen Unternehmen hindurch lückenlos nachzuvollziehen. Ob man als Unternehmen darauf spekulieren sollte, dass es so bleibt, ist eine andere Frage.