PSP
MÜNCHEN

White Paper

DSGVO — Alle froh?

Problemfälle bei der Anwendung im Unternehmensumfeld

Autor: Dr. Axel-Michael Wagner

Version 5.0
November 2019

ZUSAMMENFASSUNG

Dieses White Paper zeigt auf, dass viele alltägliche Fälle aus der Praxis mittelständischer Unternehmen mittels des DSGVO-Texts nicht eindeutig lösbar sind, was zu erheblicher Rechtsunsicherheit führt. Die Auseinandersetzung mit den Details der unternehmensspezifischen Sachverhalte und mit den verschiedenen Lesarten der datenschutzrechtlichen Regelungen ist daher ebenso unabdingbar wie die schriftliche Dokumentation dieser Auseinandersetzung. Nur so kann im Streitfall der „Beweis“ geführt werden, dass die Weichenstellungen, die dem Datenschutz-Compliance-Management-System eines Unternehmens zugrunde gelegt wurden, vertretbar waren.

PSP
MÜNCHEN

Inhalt

Versionsübersicht:
Übersicht der wesentlichen Inhaltsänderungen/ -ergänzungen

Version	Teil/Fall	Kommentierung
2.0	Einleitung	Hinweis auf Anhang ergänzt
2.0	Fall 1 und 8	Ergänzung Rechtsprechung
2.0	Fall 4 und 7	Inhaltliche Erweiterung
2.0	Fall 5	Hinweis auf Art. 6 Abs. 4 DSGVO ergänzt
2.0	Fälle 15 bis 26	Neue Fälle 15 bis 26 ergänzt
2.0	Anhang	Ergänzung eines Anhangs zur Herkunft des Daten-schutzrechts
3.0	Fälle 27 bis 32	Neue Fälle 27 bis 32 ergänzt
3.0	Fälle 1, 8 und 17	Inhaltliche Ergänzungen
4.0	Einleitung	Erster Teil der Einleitung neu verfasst
4.0	Fälle 33 bis 35	Neu ergänzt
4.0	Fälle 1, 3, 4, 6, 7, 8, 9, 10, 13, 14, 16, 17, 21, 22, 26, 27, 28, 29, 30, 31, 32	Inhaltliche Ergänzungen
5.0	Einleitung	Inhaltliche Erweiterung
5.0	Fälle 36 bis 41	Neu ergänzt
5.0	Fälle 1 bis 4, 7 bis 17, 20 bis 26, 28 bis 30, 32, 33, 35	Inhaltliche Ergänzungen

Am 25. Mai 2018 ist die EU-Datenschutzgrundverordnung (DSGVO) in Kraft getreten. Wie hat sich die DSGVO seither geschlagen? Man könnte es so formulieren: Die Büchse der Pandora wurde geöffnet. Kein Tag vergeht, an dem nicht wieder irgendjemand irgendetwas zur DSGVO zu sagen hat, seien es „Datenschutz-Experten", Aufsichtsbehörden, Berater, Aktivisten, Politiker oder – in vergleichsweise sehr geringem Umfang – Gerichte. Beinahe täglich werden Meldungen über neue Bußgelder publiziert, die Gesamtsumme geht in die Millionen. Eine Art „Bußgeldkatalog" der Datenschutzbehörden soll das bisherige Niveau der Bußgelder auf Basis eines vom Unternehmensumsatz abhängigen „Tagessatzes" wesentlich erhöhen – in Berlin wurde im November 2019 ein Bußgeld in Höhe von EUR 14,5 Mio. wegen eines fehlenden (bzw. nicht umgesetzten) Löschkonzepts verhängt. Die öffentliche Erregung hat nach der Aufregung über Klingelschilder & Co. zwar wieder Normalmaß erreicht, aber unterhalb dieser Schwelle tüftelt die juristische Fachwelt unentwegt an über 15 deutschsprachigen Gesetzeskommentierungen mit vielen tausend Seiten, an Kurzpapieren und Tätigkeitsberichten der Datenschutzbehörden, an unzähligen Artikeln, Praxishinweisen, Hypothesen und Erklärungsversuchen und an allerhand weiterem klugen Gezwitscher. Dies führt dennoch oft nicht dazu, dass Konsens erreicht wird, sondern dazu, dass das Meinungsspektrum noch breiter wird. Nach einer bitkom-Umfrage vom September 2019 sehen 95% der über befragten 500 Unternehmen die DSGVO als nicht komplett umsetzbar an, obwohl bereits ein Viertel nach eigenen Angaben die Umsetzung vollständig abgeschlossen hat. Der Bundesdatenschutzbeauftragte erklärt, die Unternehmen müssten endlich vom „Motzmodus" in den „Wettbewerbsmodus" wechseln: Datenschutzfreundliche Unternehmen seien am Markt attraktiver. So gesehen sind die vielen Milliarden, die deutsche Unternehmen zwischenzeitlich ausgegeben haben, um „compliant" zu werden (und dabei auch einen erheblichen Compliance-Rückstand aufzuholen), Marketingkosten. Wenn man denn nur genau wüsste, was man tun soll, um den Markt, den Gesetzgeber, die Aufsichtsbehörden und die Betroffenen zu erfreuen.

Der Gesetzgeber würfelt nicht – oder doch?

Der Gesetzestext der DSGVO ist abstrakt und unbestimmt. Sie erlegt dem Verantwortlichen, der personenbezogene Daten verarbeitet, ungefähr 68 verschiedene, überwiegend unscharf

formulierte Pflichten auf. Was sonst Behörden in aufwändigen Verwaltungsverfahren umsetzen müssen, enthält die DSGVO als „staatsanaloge Prüfpflichten" für den Verantwortlichen zuhauf: 3 Fairnessprüfungen, 8 Interessenabwägungen, 2 Kompatibilitätsprüfungen, 11 Geeignetheitsprüfungen, 30 Erforderlichkeitsprüfungen, 12 Angemessenheitsprüfungen, 3 Verhältnismäßigkeitsprüfungen und 13 Risikoprüfungen. Und auch die übrigen Pflichten der 68 Pflichten – wie Meldepflichten – setzen überwiegend umfangreiche unternehmensinterne Vorprüfungen bzw. Prozesse voraus.

Ebenso abstrakt und unbestimmt sind die vorangestellten 173 „Erwägungsgründe", die angeblich als „Auslegungshilfe" dienen, letztlich aber den Gesetzestext entweder erweitern oder diesem im Einzelfall sogar widersprechen. Angesichts einer solchen weiteren Verkomplizierung schon innerhalb des Gesetzestextes möchte man dem Gesetzgeber zurufen: Schreib' die Erwägungsgründe entweder in den Gesetzestext selbst oder lass' sie weg.

Die wenigen Urteile des Europäischen Gerichtshofes zum Thema Datenschutzrecht – meist noch zur Vorgängerregelung, der EU-Datenschutzrichtlinie – lesen sich wie das Orakel von Delphi, d. h. sie werfen mehr Fragen auf als sie beantworten.

Für konkrete Fallkonstellationen können mit diesen Materialien in vielen Einzelfragen keine verlässlichen Lösungen gefunden werden, wenn man einmal von den vielen allerorts publizierten „allgemeinen Hinweisen" absieht, die letztlich nur den Gesetzestext, die Erwägungsgründe oder Passagen der einschlägigen Urteile wiederholen. Zwar glauben viele, die einfache Frage „Was heißt das denn nun konkret?" beantworten zu können; tatsächlich können sie aber nur „Glaubenssätze" abliefern. Wie so oft wäre der Klügste derjenige, der sagen kann „Ich weiß (wenigstens), dass ich nichts weiß" – würde nur der Überbringer dieser schlechten Nachricht nicht hochkant hinausgeworfen. Häufig wird in Veranstaltungen auf die „schlechten Berater" geschimpft, die „Farbe bekennen", sich also festlegen müssten, welche Glaubensrichtung „richtig" ist. Diese Forderung ist bemerkenswert: Nun sollen sogar die Berater klüger als der Gesetzgeber, die Gerichte und die Behörden zusammen sein. Würden sie den sichersten – und damit aufwendigsten – Weg empfehlen, so würden sie mit Sicherheit sofort vom Hof gejagt. Man stelle sich den Berater vor, der vor der Fashion-ID-Entscheidung des EuGH geraten hätte, lieber kein Facebook-Like-Plugin zu verwenden.

- Interessengeleitete Auslegung

Unter den verschiedenen Verfechtern von Glaubenssätzen gibt es einerseits die Fraktion der „Freunde der Betroffenen"; ihre Lieblingsantworten reichen von „Man muss auf jeden Fall

eine Einwilligung einholen“ über „Sämtliche Daten müssen dann eben sofort gelöscht werden“ bis hin zu „Dann muss eben das Geschäftskonzept überarbeitet werden“. Sie sehen traditionell den „Betroffenen“ sinngemäß als „Eigentümer“ oder „Treugeber“ seiner personenbezogenen Daten an, während der „Verantwortliche“ nur „Besitzer“ oder „Treuhänder“ dieser Daten ist, also im Grundsatz mit den Daten weisungsgemäß und schonend umzugehen hat. Dabei kann sich diese Fraktion auf Erwägungsgrund 7 der DSGVO stützen, in dem es heißt: „Natürliche Personen sollten die Kontrolle über ihre eigenen Daten besitzen“. Das klingt in den Ohren mancher „Juristenforscher“ nach einem „Dateneigentum“, aber darüber hat der Gesetzgeber der DSGVO mit Sicherheit nicht nachgedacht, sondern einfach einen möglichst „knackigen“, in den Ohren einiger Interessengruppen gutklingenden und programmatischen Satz zu formulieren versucht.

Am anderen Ende der Skala gibt es die Fraktion der „Freunde der Verantwortlichen“; ihre Lieblingsantworten reichen von „Das bekommen wir schon über eine Interessenabwägung hin“ über „Es gibt immer einen legitimen Grund, Daten noch nicht zu löschen“ bis hin zu „Alles, was gewollt ist, lässt sich auch irgendwie datenschutzrechtlich umsetzen“. Für sie sind Interessen von Unternehmen im Rahmen des Datenschutzrechts essentiell: Ein Interesse an einer langen Speicherdauer, um nicht irgendwann „beweislos“ dazustehen, ein Interesse an einer „big data“-Verwendung von Daten, ein Interesse an Prozessen im Umgang mit den Betroffenen, die das Unternehmen nicht über Gebühr belasten.

Natürlich gibt es inhaltlich auch jede mögliche Position dazwischen. Die verschiedenen Gruppen von Akteuren, die im „Datenschutzmarkt“ tätig sind, lassen sich auf der Skala ungefähr wie folgt charakterisieren:

- Die rechts-, fach- und dienstaufsichtslosen – also „unabhängigen“ – Datenschutzbehörden werden mit vielen Anfragen von Betroffenen und Verantwortlichen konfrontiert und müssen sich demgemäß häufig „positionieren“. Dies geschieht neben förmlichen (Bußgeld-)Verfahren teilweise im direkten (Beratungs-)Gespräch, teilweise in den jährlich vorzulegenden Tätigkeitsberichten und teilweise in den zwischen den Datenschutzbeauftragten der Länder abgestimmten Kurzpapieren der Datenschutzkonferenz (DSK). Daneben versuchen die Datenschutzbehörden, den bisherigen „Wissensschatz“ über die Auslegung der Vorgängerrichtlinie der DSGVO, der Datenschutzrichtlinie, und des vormaligen Bundesdatenschutzgesetzes so gut wie möglich „hinüberzuretten“ in die DSGVO-Zeit. Ähnliches passiert auf europäischer Ebene bei der Übernahme der „guidance“ der vormaligen Artikel-29-Datenschutzgruppe der EU-Länder im Rahmen der Fortführung durch den Europäischen Datenschutzausschuss. Die Grundlinie der

Datenschutzbehörden ist es dabei, „datenschutzfreundlich“ zu sein und einerseits auf die Kontinuitäten zum alten Recht hinzuweisen („das war doch alles schon immer so“), andererseits aber auf die strengeren Maßstäbe der DSGVO hinzuweisen („da hat jetzt der Gesetzgeber aus gutem Grund die Zügel noch stärker angezogen“). Die DSGVO wird hier wortgetreu (weit) und rigoros angewendet, juristische „Kunstgriffe“ bzw. feinziselierte Argumentationen fehlen meist. Zudem sind die Datenschutzbehörden personell unterbesetzt und die beantragten zusätzlichen Stellen werden von den Landtagen nur teilweise bewilligt, was wiederum als europarechtswidrig gewertet wird („Geld hat man zu haben“). Nicht auszudenken, was in der EU passieren würde, wenn es zu jedem EU-Bürger einen Datenschutzbehörden-Mitarbeiter gäbe, der ihm stets auf Schritt und Tritt, auf Facebook und Twitter, im geschäftlichen und privaten Umfeld folgt. Wäre eine solche Kontrolldichte – der Gesetzgeber möchte ja, dass seine Gesetze möglichst lückenlos eingehalten werden – datenschutzrechtlich überhaupt zulässig? Wer wissen möchte, welche (offenen) Fragen eine Datenschutz-Aufsichtsbehörde so stellt, was sie sich dabei (insgeheim) denkt bzw. welche Erwartungshaltung sie an die Antworten hat, und wie mittlere und große Unternehmen dabei so abschneiden, dem sei der Abschlussbericht zur „Querschnittsprüfung des LfD Niedersachen von 50 Unternehmen zur Umsetzung der seit dem 25. Mai 2018 unmittelbar geltenden DSGVO“ vom November 2019 ans Herz gelegt. Es kann nicht überraschen, dass diese Prüfung – die sehr auf die formalen Anforderungen der DSGVO konzentriert war – die größten Probleme im Bereich der Datenschutz-Folgenabschätzung und der technisch-organisatorischen Maßnahmen ausmachte. Wenn man sich die dortigen Ausführungen zur Erwartungshaltung bezüglich der Artikel 24, 32 und 35 DSGVO durchliest, stellt man fest, dass dies echte „Knaller“ sind, die kaum jemand ohne „Millionenaufwand“ zur Zufriedenheit einer datenschutzfreundlichen Aufsichtsbehörde umsetzen kann. Möglicherweise schlummert aber noch ein größeres Problem in der Bestimmung der „richtigen“ Legitimationsgrundlage für die einzelnen Verarbeitungstätigkeiten, die natürlich im Rahmen dieser Prüfung nicht im Einzelnen verifiziert wurden.

- Die „Fachwelt“ versucht, in Kommentaren, Fachartikeln und verstreuten Internet-Schnipseln (Blogs, Tweets, Kurzhinweise etc.) neben mehr oder weniger umsetzbaren Praxistipps (die doch oft nur aus Wiederholungen der Primärtexte bestehen) auf die vielen Widersprüche und für die Praxis absurden (oder besser: absurd teuren bzw. aufwendigen) Folgen der DSGVO-Regelungen hinzuweisen. Neben vielen Warnungen, was alles zukünftig noch wie eingeordnet werden könnte (z. B. als gemeinsam Verantwortliche), versucht die Wissenschaft, der DSGVO einen dogmatischen Unterbau – sozusagen ein systematisches Grundgerüst – zu verpassen. Der Gesetzgeber wird sich

doch bei all dem irgendetwas gedacht haben, außer nur Google und Facebook an die Kandare nehmen zu wollen (was allerdings bislang nicht so gut funktioniert)! Ein Beispiel hierfür ist die Diskussion darüber, welches „Schutzgut" die DSGVO überhaupt schützt – die dort angegebenen „Rechte und Freiheiten der Betroffenen" halten verschiedene Autoren für zu vage und daher konkretisierungsbedürftig. Der DSGVO wird bisweilen sogar vorgeworfen, das Gegenteil von dem zu erreichen, was sie angestrebt hat – nämlich eine totale Kontrolle jeglichen Verhaltens von Betroffenen aus der Perspektive des Datenschutzes im Gewand eines paternalistischen „Betroffenenschutzes". So wird viel im Kaffeesatz gelesen, Grundrechte werden gewälzt und ein in sich stimmiges, sinnhaftes Rechtssystem wird „herbeikonstruiert", über das sich aber vor Erlass der DSGVO nie jemand ernsthaft Gedanken gemacht hat. Insoweit gleicht es einer „Sinnsuche im Unsinnigen". Insgesamt fällt dabei auf, dass die Fachwelt häufig wenig fallzentriert, sondern vornehmlich abstrakt bzw. abgehoben argumentiert. Dieses Abstraktionsniveau mag den Innenraum der vielen „Datenschutz-Dichter und -Denker" beflügeln, produziert aber oft keine überzeugenden bzw. umsetzbaren Lösungen für den Alltag, sondern bleibt im Ungefähren.

- Die Gerichte sind bekanntlich die einzigen Institutionen, welche verbindlich entscheiden können, wie das Datenschutzrecht anzuwenden ist – neben dem Gesetzgeber selbst, der aber noch nie (im Sinne einer „agile legislation") geneigt war, die Lückenhaftigkeit und Praxisuntauglichkeit seiner eigenen Gesetze durch Konkretisierungen auszumerzen. Allerdings sind auch Richter nur Menschen, die sich zudem nicht ausschließlich mit Datenschutzrecht beschäftigen, sondern für die dies nur ein Thema von vielen anderen ist. Es war nie das Ziel oder die Aufgabe von Gerichten, dogmatische Grundlagenarbeit zu leisten. Gerichte müssen immer nur sagen, was nicht geht, aber nie, wie es gegangen wäre – es sei denn, in einem Sachverhalt wurde zufälligerweise mal alles richtig gemacht. Gerichte sind ja keine Rechtsberater und müssen dazu noch oft die Rolle des „Notgesetzgebers" ausfüllen. Entsprechend neigt die „Fachwelt" – wie beim Gesetzestext selbst – dazu, in Urteile unglaublich viel über den konkreten Fall „Überschießendes" hineinzulesen, worüber die Richter sich aber beim „Verfertigen" des Urteils mit Sicherheit keine Gedanken gemacht haben. Und so haben diverse Richter in Sachen DSGVO schon verschiedene „Rechtssätze" aufgestellt, die von den beiden Lagern – den Freunden der Betroffenen und den Freunden der Verantwortlichen – jeweils entweder triumphierend (und damit verabsolutierend) oder trotzig (und damit relativierend) aufgenommen werden. Da kann es nicht überraschen, dass beispielsweise das überaus kryptische Facebook-Fanpage-Urteil des EuGH nach einer ersten Urteilsbesprechung „auf mindestens drei verschiedene Weisen" gedeutet werden

kann. Die Probleme, welche die oben bereits angesprochene Fashion-ID-Entscheidung aufwirft, sind nicht weniger relevant. Die Gerichte machen also alles vordergründig einfacher, indem sie verbindlich Recht sprechen, und hintergründig komplizierter, indem ihre Urteile mehr Fragen aufwerfen, als sie beantworten. Hinzu kommt noch, dass der Europäische Gerichtshof seinen Entscheidungen im Bereich Datenschutz häufig die „Grundregel" voranstellt, dass Datenschutz „das" Schutzinstrument für (sämtliche?) Rechte und Freiheiten der EU-Bürger sei, sodass man sich auch ohne weiteres Lesen schnell denken kann, wie die Entscheidung ausgegangen ist. Eine Entscheidung zu „weniger Datenschutz" scheint da kaum vorstellbar zu sein. Und ganz allgemein gesprochen sind die Gerichte meist weder in Sachen Datenschutz noch in Sachen Technikverständnis besonders spezialisiert – es gibt zwar an den deutschen Gerichten beispielsweise (spezialisierte) „Kammern für Baulandsachen", aber bislang keine „Kammern für Datenschutz" und erst Recht nicht für IT-Verständnis.

- Der Gesetzgeber macht nicht viel im Bereich Datenschutz, denn er hat andere Baustellen. Nebenbei muss eigentlich noch eine große Zahl an Bundes- und Landesgesetzen an das neue Datenschutzrecht angepasst werden, was aber eher „technischen" Folgeänderungen zuzuordnen ist – auch dieses Projekt zieht sich wie Kaugummi. Ohnehin ist der bundesdeutsche Gesetzgeber letztlich nicht mehr gesetzgebungsbefugt. Jede Regelung, die der deutsche Gesetzgeber im Rahmen von „Öffnungsklauseln" der DSGVO erlässt, wird früher oder später von irgendeiner Interessengruppe als „europarechtswidrig" gebrandmarkt. Damit wird es unsicher, sich darauf zu berufen. Wenn die (Datenschutz-)Behörden von einer Europarechtswidrigkeit ausgehen, müssen sie – da weicht das Europarecht sehr vom deutschen (Verfassungs-)Recht ab – die entsprechende bundesdeutsche oder landesgesetzliche Norm nicht anwenden. Unabhängig davon rückt auf europäischer Ebene die E-Privacy-Richtlinie, die das Datenschutzrecht im Online-Sektor spezifischer regeln und gemeinsam mit der DSGVO in Kraft treten sollte, in immer weitere Ferne. Das wiederum wirft Folgeprobleme in Bezug auf die in Umsetzung der vormaligen E-Privacy-Richtlinie erlassenen Rechtsvorschriften auf, die sich angeblich nun nicht mehr an der E-Privacy-Richtlinie, sondern an der DSGVO messen lassen müssen.

- Die Verantwortlichen und deren Auftragsverarbeiter lassen sich im gesamten Spektrum zwischen „versuchter Vorbildlichkeit" und „Ignoranz" einordnen. Auf der einen Seite entbrennt ein Wettbewerb darum, wer (bzw. welcher betriebliche Datenschutzbeauftragte) das längste und detaillierteste Verarbeitungsverzeichnis vorweisen kann. Die

Muster werden immer ausgefeilter und die Mustergültigkeit der Datenschutz-Compliance-Organisation auch, bis man den Wald vor lauter Bäumen nicht mehr sieht. Es werden softwaregestützt Prozesslandschaften („process discovery", „process inventory", Daten-Bestände („data discovery", „data inventory"), Zweckverzeichnisse („purpose discovery", „purpose inventory"), Risikolisten („privacy risk discovery", „privacy risk inventory"), Risikoschleusen („privacy risk control gateways"), Visualisierungswerkzeuge, Datenqualitätswerkzeuge („data quality assurance tools") und Metadaten etabliert und gepflegt. Wer aber einmal versucht hat, ein „gewachsenes" SAP-System von Grund auf auseinanderzunehmen und datenschutzkonform wieder aufzubauen, der muss deutlich mehr leisten als nur „hippe Begriffe" zu kreieren. Auf der anderen Seite stehen diejenigen Unternehmen, die kühl mit der geringen (behördlichen) Kontrolldichte kalkulieren und hoffen, dass der Kelch möglichst lange an ihnen vorbeigeht, und wenn er doch kommt, dass sie sich dann schon irgendwie herauslavieren können. Letzteres ist insbesondere (noch) der Trend im deutschen Mittelstand, der schon „irgendwie von diesem neuen Datenschutzrecht gehört" und auch schon einen Klauselgenerator für Website-Datenschutzerklärungen verwendet hat, weil man ja doch eine Datenschutzerklärung haben sollte. Dazu ein externer Datenschutzbeauftragter für 120 Euro im Monat. Die moralische Rechtfertigung für solche „Potemkin'schen Datenschutzdörfer" wird bisweilen darin gesucht, dass „ich das Unternehmen ja nur noch ein paar Jahre führe, und dann soll sich mein Nachfolger damit herumschlagen".

- Die Betroffenen wiederum lassen sich dem gesamten Spektrum zwischen „Ich klick sowieso immer auf zustimmen" und „Den mach ich mit dem Datenschutzrecht fertig" einordnen. Letzteres wird zwangsläufig auch immer mehr zur Spielwiese der Berater: Wenn ein Anwalt eine Pflichtverletzung begeht, weil er einem Geschäftsführer einer Gesellschaft nicht empfiehlt, sein Amt niederzulegen, um in einem Zivilprozess nicht als Partei, sondern als Zeuge aussagen zu können, dann könnte es auch pflichtwidrig sein, in einer Abfindungsauseinandersetzung zwischen Arbeitgeber und Arbeitnehmer nicht zu empfehlen, den Arbeitgeber noch ordentlich mit datenschutzrechtlichen Auskunftsansprüchen zu „piesacken". Dazwischen liegt irgendwo der mündige Bürger, der um seine Rechte weiß und diese in Situationen ausüben würde, in denen es ihm wirklich darauf ankommt – was in der Praxis allerdings (noch) eher selten der Fall ist, vermutlich weil mündige Bürger noch ganz andere Probleme als ihre datenschutzrechtlichen Betroffenenrechte haben (und bisweilen auch gar nicht wissen wollen, was mit ihren Daten noch so alles angestellt wird). Das englische „ignorance is bliss" trifft ohnehin die Situation recht gut: Wenn man die bisherigen Skandalmeldungen, wie viele Millionen und Milliarden Datensätze – von Kreditkartendaten bis zu Gesundheitsdaten

– offen oder halboffen herumliegen, extrapoliert, dann will man sich gar nicht ausmalen, wer mit guten Werkzeugen aus dem Darknet noch viel mehr herausholen könnte unter Ausnutzung von Sicherheitslücken, die erst übermorgen publik werden.

Damit wären wir wieder am Anfang, beim größten Problem der DSGVO: Keiner weiß, wie es wirklich sein soll, aber jeder denkt, er wisse es. Das liegt schlicht daran, dass es ein definiertes „Sollen" nicht gibt: Die DSGVO ist eben nur so gut, wie sie ist, und zudem „wechselwirkt" sie mit vielen anderen (insbesondere nationalen) Rechtsquellen – etwa im Bereich der Aufbewahrungspflichten –, die nicht mit Blick auf die DSGVO erschaffen wurden.

➢ Parallelwelten zur DSGVO

Nicht umsonst werden für betriebliche Datenschutzbeauftragte und Zertifizierungsstellen „umfassende Fachkompetenz in technischer und juristischer Hinsicht" vorgegeben; Vorgaben, die der DSGVO-Gesetzgeber jedenfalls nicht erfüllen musste. Die Gesetzesgeschichte der DSGVO selbst kann vielmehr, wenn man die Berichte über deren Zustandekommen verfolgt hat, nur als „traurig" bezeichnet werden – viel Ideologie (bzw. Politik), aber wenig Sachverstand und wenig tiefgehendes Verständnis für die Komplexität „da draußen" und für Zusammenhänge zwischen verschiedensten Themenkomplexen sind in den Gesetzestext eingeflossen. Der beste politische Kompromiss ist bekanntlich der, bei dem sich jede Interessengruppe „im Text wiederfindet", sprich, den Text im Sinne der von ihr vertretenen Interessen lesen kann. Dabei leisten die Erwägungsgründe tatsächlich gute Dienste, erschweren aber dem Rechtsanwender das Leben und werfen die ganz grundsätzliche Frage auf, was das Ziel eines Gesetzestextes sein sollte. Und so wachsen die über die DSGVO verfassten Sekundär-, insbesondere Fachinformationen seit der ersten Stunde in exponentiellem Tempo zu einem Informationsberg an, auf den der datenschutzrechtliche Sisyphus jeden Tag seinen Stein hinaufzuschieben versucht – der dann täglich wieder hinabrollt. Niemand weiß, wie viele Stunden wie viele Personen sich inner- oder außerhalb wie vieler Unternehmen und Organisationen schon mit DSGVO-Fragen beschäftigt haben und was alleine das gekostet hat.

Da die Regelungen der DSGVO überwiegend hoch abstrakt – euphemistisch wird häufig das Wort „technikneutral" verwendet – und nicht konkret formuliert sind, gehen also nun verschiedene Bemühungen dahin, die DSGVO in ein in der Praxis handhabbares Regelwerk „umzumünzen". Diese Bemühungen übersteigen das Kommentieren des Gesetzestextes, etwa in Form der Kurzstellungnahmen der Datenschutzkonferenz oder in den großvolumigen Kommentaren namhafter deutschsprachiger Datenschutzrechtler, bei Weitem:

- Die Datenschutzbehörden versuchen etwa, mit dem „Standard-Datenschutzmodell“ (SDM) die datenschutzrechtlichen Vorgaben über eine begriffliche Zwischenebene von Schutz- bzw. Gewährleistungszielen des technischen Datenschutzes in technische und organisatorische Maßnahmen zu „überführen“. Das Standard-Datenschutzmodell liegt seit November 2019 als Version 2.0 vor und gliedert sich in ein „Methodik-Handbuch“ und einzelne, darauf aufbauende „Bausteine“ zu bestimmten Themen. Die meisten der dort genannten „Gewährleistungsziele“ – die etwas anders als die in Art. 5 DSGVO wiedergegebenen Grundprinzipien lauten – finden sich als klassische IT-Sicherheitsziele auch im IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wieder, dessen Abschnitt zum Thema Datenschutz die Vorgabe enthält, dass die Nichtberücksichtigung des Standard-Datenschutzmodells begründet werden muss. Wer sich also im Rahmen des technischen Datenschutzes beispielsweise an die ISO 27701 anlehnt, muss nach den IT-Grundschutz-Vorgaben darlegen, warum diese Norm – außerhalb des Standard-Datenschutzmodells – die Anforderungen der DSGVO abdeckt. Inhaltlich ist allerdings die „Stoßrichtung“ des BSI-Grundschutzkatalogs die Sicherheit der IT des Unternehmens, während das Standard-Datenschutzmodell Risiken aus der Perspektive des (von der DSGVO geschützten) Betroffenen und dessen personenbezogene Daten beleuchtet. Mit dem Standard-Datenschutzmodell kann in diesem Sinne im Rahmen von Planung, Einführung und Betrieb von Verarbeitungstätigkeiten das Risiko einer Verarbeitung personenbezogener Daten gemessen und durch zu ermittelnde konkrete technische und organisatorische Maßnahmen auf ein (für den Betroffenen und damit auch für den Verantwortlichen) „tragbares“ Maß reduziert werden. Dies ist Teil des sog. Datenschutzmanagement-Prozesses, der „als dauerhafter, zyklischer Prozess“ nach dem PDCA-Vorgehen („plan, do, check, act“) der kontinuierlichen Verbesserung eingerichtet werden und bei der Einhaltung der Rechenschafts- und Nachweispflichten helfen soll (s. dazu auch unten Fall 37). In der „Sprache“ der Entscheidungen des Europäischen Gerichtshofes spielt die Nomenklatur des Standard-Datenschutzmodells allerdings bislang eine eher untergeordnete Rolle. Für den Europäischen Gerichtshof ist die DSGVO ein Gesetz, welches das Grundrecht auf Datenschutz (Art. 8 der EU-Grundrechtecharta) aufgrund der in Art. 8 Abs. 2 der EU-Grundrechtecharta aufgenommenen (Gesetzes-)Vorbehalt einschränkt („*Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden*“). Dies kennzeichnet – auch sprachlich – den Ausgangspunkt der Entscheidungen des Europäischen Gerichtshofes in Sachen Datenschutz, nicht „Gewährleistungsziele“. Ungeachtet der Frage, ob das Standard-Datenschutzmodell sinnvoll

und praktikabel ist, beschleicht einen hier der Argwohn, dass die Datenschutzbehörden sich – wie im Steuerrecht die Steuerbehörden über „Rundschreiben", „Erlasse" und (natürlich) Gesetzesentwürfe – „ihr" Recht am liebsten selbst schaffen würden, das sie dann vollziehen können.

- Daneben werden im Rahmen von Zertifizierungsverfahren, welche die DSGVO abstrakt regelt, die datenschutzrechtlichen Vorgaben durch Kriterienkataloge in „prüffähige, normative Kriterien", die ein Verantwortlicher erfüllen muss, übersetzt. Ein „Konformitätsbewertungsprogramm" beschreibt dann jeweils die Anforderungen, Regeln und Prüfverfahren, die anzuwenden sind, um die mit der Zertifizierung verbundene (Konformitäts-)Aussage auf wissenschaftlich rückführbare und systematische Weise treffen zu können. Bei der Spezifikation eines solchen Konformitätsbewertungsprogramms soll sichergestellt werden, dass verschiedene Prüfer zum gleichen Ergebnis der Konformitätsbewertung kommen. Hier wird also ein ganz anderer Bestimmtheitsmaßstab angewandt als innerhalb der DSGVO selbst. Eine datenschutzrechtliche Zertifizierung eines IT-Anbieters beispielsweise – so wie sie derzeit als Anwendungsfall entwickelt wird – umfasst anhand von konkreten Einzelvorgaben die Prüfung der Dokumentation, die Durchführung von Befragungen, die Überwachung von Vorgängen, technische Tests, die Beurteilung von Entwicklungen, Asset- und Vor-Ort-Prüfungen, jeweils in Bezug auf Verträge, Prozesse, Diensteigenschaften, Infrastruktur- und Softwarekomponenten und Mitarbeiter. Man könnte auch sagen, eine forensische Untersuchung des Unternehmens insgesamt. Das funktioniert nur, wenn konkretisierende Weichenstellungen vorgenommen werden, die der Gesetzgeber gerade nicht vorgenommen, sondern den Gerichten überlassen hat.

- Der IDW-Prüfungshinweis 9.860.1 wiederum konkretisiert auf seine Weise – außerhalb der Regelungen der DSGVO für die Zertifizierung – die Anforderungen an die Prüfung eines Datenschutz-Compliance-Management-Systems (und damit auch die inhaltliche Voraussetzungen für ein solches).

- Verschiedene Verhaltensregeln werden auf Basis von Art. 40 Abs. 2 DSGVO von den dort genannten „Verbänden und anderen Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten", entwickelt. Der Europäische Datenschutzausschuss hat hierzu im Juni 2019 Empfehlungen zum Prozess der Abstimmung solcher Verhaltensregelungen mit den Aufsichtsbehörden herausgebracht. Als Beispiel sei der Code of Conduct zum Einsatz DSGVO-konformer Pseudonymisierung der „Fo-

kusgruppe Datenschutz“ der „Plattform Sicherheit, Schutz und vertrauen für Gesellschaft und Wirtschaft“ genannt. Hiernach muss zunächst ein „Fachverantwortlicher für Pseudonymisierung“ ernannt werden, der nicht mit dem Datenschutzbeauftragten identisch sein darf. Ansonsten beschäftigt sich der Code of Conduct mit der Festlegung der Pseudonymisierungsmethode anhand von Risiko, Zweck, Kontext und Anzahl der Verarbeitung. Weitere Abschnitte befassen sich mit einem risikoadäquaten Rechte- und Rollenkonzept, mit Vorgaben für die Re-Identifizierung, einem Reaktionsplan bei unbeabsichtigter oder unrechtmäßiger Aufhebung der Pseudonymisierung, Dokumentation und technischen Fragen. Teils wird auf die Anforderungen der DSGVO verwiesen, teils eigene Anforderungen aufgestellt. Man kann sich vorstellen, in welchem unübersichtlichem Gestrüpp von Verhaltensregeln sich ein Verantwortlicher wiederfinden kann, wenn in Zukunft verschiedenste solcher Regelwerke „längs und quer“ zur DSGVO miteinander wetteifern.

Es dürfte also nicht verwundern, wenn demnächst irgendjemand das Projekt „Mapping verschiedener Zertifizierungs- und Prüfungskriterien“ angeht – hoffentlich nicht nur ein Vergleich der einzelnen Vorgaben im Verhältnis zueinander, sondern jeweils auch im Verhältnis zur DSGVO selbst. Und dann sollte es natürlich nicht überraschen, wenn diesbezüglich in der Zukunft die Position vertreten wird, dass einige dieser „Sekundärnormensysteme“ an der einen oder anderen Stelle (möglicherweise) nicht mit der DSGVO kompatibel sind – so wie auch in der Vergangenheit schon einige Anleitungen zum Aufbau von Compliance-Management-Systemen von Juristen als nicht kompatibel mit dem Organhaftungsrecht (§ 93 AktG) bezeichnet wurden, ohne dass es jemand „wirklich weiß“.

Neben derartige Bemühungen um Präzisierung seitens verschiedener Organisationen treten Versuche, das Datenschutzrecht in der Praxis großer Unternehmen „handhabbar“ zu machen. Die Entwicklung einer solchen „best practice“, verbunden mit den obligatorischen *„key performance indexes“* („KPIs“) zur Effizienzmessung des Erfolgs eines Datenschutzmanagementssystems, dient vordergründig dem Zweck, Komplexität zu reduzieren. Selbst der Europäische Datenschutzausschuss hat in Empfehlungen vom November 2019 zum Thema *„privacy by design/by default“* die Verwendung von KPIs propagiert und nur als „Alternative“ die Erläuterung des Verantwortlichen, warum eine Maßnahme effektiv ist, genannt:

„controllers must be able to demonstrate that they have implemented measures and safeguards to achieve the desired effect in terms of data protection. To do so, the controller may determine appropriate key performance indicators to demonstrate compliance. Key performance indicators may include metrics to demonstrate the effectiveness of the measures in

question. Metrics may be quantitative, such as level of risk, reduction of complaints, reduction of response time when data subjects exercise their rights; or qualitative, such as evaluations of performance, use of grading scales, or expert assessments. Alternatively, controllers may provide the rationale behind their assessment of the effectiveness of the chosen measures and safeguards."

Solche Ansätze, die komplexe Input-Informationen in einfache Output-Informationen übersetzen, haben naturgemäß ihre Tücken. Nehmen wir das Beispiel Löschpflicht und Löschkonzept. Hier werden personenbezogene Daten in Schutzklassen eingeteilt sowie Löschklassen und Standardfristen gebildet. Und doch kollidieren derartige Versuche prinzipiell mit der vom DSGVO-Gesetzgeber grundsätzlich beabsichtigten Einzelfallbetrachtung. So hat zwar die DIN 66398 lobenswerterweise schon vor Einführung der DSGVO versucht, eine „Rasterung" von Löschregeln zu definieren, in deren Rahmen dann z. B. die Datenfelder einer ERP-Software wie SAP berücksichtigt werden können. Doch wenn man jedes Datenfeld einzeln analysiert, stellt man fest, dass mit einer solchen Rasterung Datenschutzverstöße vorprogrammiert sind, weil die Reduzierung der Komplexität auf Kosten der Genauigkeit im Einzelfall geht. Also wird man doch versuchen, hunderten von Datenfeldern in SAP jeweils einzelne Löschfristen zuzuweisen. Hinter jeder einzelnen Löschfrist steht dann eine Abwägung zwischen Aufbewahrungspflichten, Auskunftspflichten gegenüber Behörden und sonstigen Stellen, Verjährungsfristen, Aufbewahrungsinteressen und sonstigen Interessen des Verantwortlichen einerseits und „typisiertem" Löschinteresse des Betroffenen (das auch in ein „Recht auf Nichtlöschung" umschlagen kann) andererseits. Und wenn ein Datenfeld „Abwesenheit" sowohl „Urlaub" als auch „Krankheit" als auch „Mutterschutz" als Dateninhalt aufweisen kann, muss vielleicht noch weiter differenziert werden. Gerade Aufbewahrungs- und Auskunftspflichten sind in den verschiedensten Gesetzen mit unterschiedlicher Zweckrichtung, unscharfen Abgrenzungen der aufzubewahrenden oder zu beauskunftenden Informationen sowie unklaren Fristenden (insbesondere bei Auskunftspflichten) geregelt. Man merkt dann schnell, dass sich der Gesetzgeber darüber jedenfalls keine Gedanken gemacht hat. Letztlich erhöht sich daher die Komplexität und das Risiko von Fehlbeurteilungen weiter, wenn sich zur angeordneten Einzelfallbetrachtung nun auch noch verschiedene Ebenen der Rasterung (Kategorisierung) von Fallgestaltungen gesellen, die den Einzelfällen mal mehr, mal weniger gerecht werden. Mit anderen Worten: Je mehr Betrachtungsebenen, desto mehr Konfliktpotenzial zwischen den Ebenen.

Gleich mit welchen Mitteln nun aber eine möglichst hohe Präzision (bzw. Gesetzestreue) erreicht wird – hierzu zählt auch das oben erwähnte Beispiel „Code of Conduct" als Instrument der „konkretisierenden Selbstbindung" einzelner Wirtschaftszweige –, bleibt sie doch

stets eine „Pseudo-Präzision“ durch nicht-legislative und nicht-judikative Stellen. Denn sämtliche Versuche, die DSGVO zu präzisieren, müssen die unumstößliche Tatsache ignorieren, dass nur der Gesetzgeber und der Europäische Gerichtshof die DSGVO verbindlich präzisieren können und eben vieles vom Gesetzgeber nicht im Detail (in dem bekanntlich der Teufel liegt) durchdacht wurde. Entweder außerhalb der DSGVO formulierte Vorgaben wiederholen nur die DSGVO (in anderen Worten), dann sind sie eigentlich überflüssig, oder sie formulieren Anforderungen, die sich nicht aus der DSGVO ergeben, dann ist offen, ob die DSGVO dabei richtig interpretiert wurde. Der Thüringer Landesbeauftragte für Datenschutz formuliert dementsprechend – wenig tröstlich für den Rechtsanwender – in seinem Tätigkeitsbericht 2018 im Zusammenhang mit der Durchführung von Datenschutz-Folgenabschätzungen:

„Werden bestehende Methoden oder Standards eingesetzt, ist allerdings zu beachten, dass die Anforderungen der DS-GVO immer vorrangig zu beachten sind.“

Deshalb dürfte eigentlich auch die (wirtschaftliche) Motivation verantwortlicher Unternehmen, sich freiwillig den Anforderungen datenschutzrechtlicher „Parallelwelten“ zu unterwerfen, begrenzt sein, weil damit das Risiko verbunden ist, mit erheblichem finanziellen Aufwand Normen einzuhalten, deren Einhaltung der Gesetzgeber selbst vielleicht gar nicht eingefordert hat („Über-Compliance“). Aber der Trend der zunehmenden Aufstellung von (Sekundär-)Normen, Leitlinien, Prüfungs- und Zertifizierungs-„Programmen“ durch verschiedenste Institutionen und Organisationen in den verschiedensten „Compliance“-Bereichen (obwohl Compliance doch ursprünglich nur die systematische Einhaltung der geltenden Gesetze meint) schafft nicht nur eine demokratisch nicht legitimierte Pseudo-Gesetzeswelt, sondern auch den „Gruppenzwang“ („peer pressure“) zu deren Einhaltung. Der Gesetzestext reicht also „irgendwie“ nicht aus – man stelle sich einmal zum Vergleich „Leitlinien des ADAC für Compliance im Straßenverkehr“ vor, deren Einhaltung dann, weil man sich die Nichteinhaltung schlichtweg „nicht leisten kann“, zum guten Ton gehört. Und pikanterweise birgt eine derartige „Pseudo-Präzisierung“ umgekehrt die Gefahr, dass selbst Gerichte – die Richter sind ja meist keine Datenschutz-Experten – in der Hektik des Alltags vor dem Hintergrund des unbestimmten und damit schwer verständlichen Gesetzestextes eine bestimmte Interpretation der DSGVO – durch wen auch immer „vorgedacht“ – unreflektiert als „maßgeblich“ unterstellen. Beispiele gibt es hierzu schon genügend – aber auch Verteidiger, die solche Schnellschüsse als Ausdruck tiefgreifender Durchdringung der Materie interpretieren. Im Strafrecht gilt zwar seit jeher, dass wenn sich der Gesetzgeber nicht präzise (d. h. „bestimmt“) ausdrücken kann, dies nicht zu Lasten des Gesetzesadressaten geht. Im Datenschutzrecht aber ist das (bislang) nicht so: Man wird immer jemanden finden können, der

den dehnbaren Gesetzestext noch weiter dehnt und dessen Unbestimmtheit als – „selbstverständlich (verfassungs-)rechtlich zulässigen" – Vorteil propagiert.

- „Quidquid agis, prudenter agas, et respice finem"

Was den Gesetzgeber selbst anbelangt, mehren sich die Zweifel, ob den Akteuren, die an der DSGVO-Gesetzgebung mitwirkten, überhaupt bewusst war, welche Bandbreite an Sachverhalten sie mit der DSGVO regeln. Vordergründig ging es darum, „die großen internationalen Datenkraken" in den Griff zu bekommen – Wer wollte einer solchen politischen Absicht widersprechen? Eine Simulation im Vorfeld in einer kleineren (Test-)Umgebung, um die praktischen Folgen der DSGVO und ihrer begrifflichen Unbestimmtheiten vorab abschätzen zu können, ist gleichwohl nicht überliefert. Das „Arbeitsdokument der Kommissionsdienststellen" zur „Zusammenfassung der Folgenabschätzung" vom Januar 2012 vergleicht lediglich die Optionen „weiche Maßnahmen", Aktualisierung der Datenschutzrichtlinie 1995 und „detaillierte Rechtsregelung auf EU-Ebene". Dabei wird neben den Kosten für die Benennung eines betrieblichen Datenschutzbeauftragten (EU-weit EUR 320 Mio. pro Jahr) darauf hingewiesen, dass die „verstärkten Datenschutzregeln mit einigen Zusatzkosten für die Einhaltung verbunden sein dürften, besonders wenn es sich um für eine risikobehaftete Datenverarbeitung Verantwortliche handelt". Allerdings „dürften" diese (unbezifferten) Kosten „angesichts des Nutzens und der Einsparungen beim Verwaltungsaufwand in Höhe von mehr als EUR 2,3 Mrd. pro Jahr verhältnismäßig sein". Ob solche auf unsicherer Informationsgrundlage prognostizierten Einsparungen beim Verwaltungsaufwand später noch einmal mit der Realität abgeglichen werden, ist eher zu bezweifeln: Jedenfalls ist nicht ersichtlich, dass der EU-Gesetzgeber eine Folgenabschätzung in der Sache selbst – Norm für Norm – betrieben hätte, die er aber nun umgekehrt mit der DSGVO jedem Unternehmen (insbesondere, aber nicht nur, als Datenschutz-Folgenabschätzung in undefinierten „Hochrisikosituationen") ins Stammbuch schreibt. Das Statistische Bundesamt jedenfalls hatte 2015 die Mehrkosten für Unternehmen, die sich aus ausgewählten vier von 30 Artikeln ergaben (insbesondere die Erteilung von Pflichthinweisen an die Betroffenen), mit EUR 1,5 Mrd. im ersten Jahr und EUR 1 Mrd. pro Folgejahr veranschlagt. Die daraufhin angestrebten Erleichterungen für Kleinstunternehmen ließen sich jedoch politisch in Brüssel nicht durchsetzen. Warum nur diese 30 Artikel einer Prüfung unterzogen wurden, andere Pflichten aber nicht, weiß heute niemand mehr. Letztlich wurden die dahinter stehenden Bedenken beiseite gewischt, wobei die grundsätzliche Frage, wie viel Sachverstand in geordneter Form erfolgreich in die DSGVO eingebracht wurde, mittlerweile ohnehin nur noch „rechtshistorische" Bedeutung hat. Die verfügbaren „Insider"-Berichte über das Gesetzgebungsverfahren zur DSGVO rücken deren Entstehung in kein gutes Licht. So oder so: Die Umsetzung der DSGVO bei europäischen und außereuropäischen Unternehmen hat immense Kosten produziert und wird

diese auch weiter produzieren; die Dimension dieser Kosten wurde vorher weder genauer abgeschätzt noch hat sie relevante Spuren im Verordnungstext hinterlassen und sie spielt jetzt, nach dem Inkrafttreten, auch keine Rolle mehr.

Was diese programmatische Unbestimmtheit der DSGVO konkret bedeutet, lässt sich an der Entwicklung eines der vielen Problemfälle des Datenschutzrechts zeigen: Vor zwei Entscheidungen des EuGH und des Bundesgerichtshofs in den Jahren 2016 und 2017 war höchst unklar, ob eine dynamische IP-Adresse für den Betreiber einer Website, der diese Daten in einem Logfile speichert, ein personenbezogenes Datum darstellt. Es gab viele Argumente dafür wie dagegen und man hätte ebenso gut die Würfel werfen können. Sowohl eine „Ja"- als auch eine „Nein"-Entscheidung wäre stringent begründbar gewesen; ein Leser hätte wohl gedacht, warum man diese Angelegenheit angesichts der Klarheit der Entscheidung überhaupt ausstreiten musste. Dennoch lautete – wie so oft – die Antwort des EuGH: „Es kommt darauf an", was die Sache nicht einfacher machte. Der Bundesgerichtshof, der die Grundsatzentscheidung des EuGH auf den Fall umzusetzen hatte, erklärte lakonisch: Ein Website-Betreiber, der eine dynamische IP-Adresse eines Besuchers speichert, kann im Falle einer eingetretenen Schädigung eine Strafanzeige (wegen Computersabotage) erheben oder im Falle einer drohenden Schädigung die zur Gefahrenabwehr zuständigen Behörden informieren, und die Staatsanwaltschaft bzw. die Gefahrenabwehrstelle kann über die Auskunftspflicht des Providers den Inhaber des Anschlusses zur Tatzeit ermitteln. Damit würden die IP-Adresse und die Identität des Anschlussinhabers „zusammengeführt", weshalb die dynamische IP-Adresse ein personenbezogenes Datum sei. Der Anschlussbetreiber „hinter" der dynamischen IP-Adresse ist damit aus der Perspektive des Website-Betreibers bereits deshalb identifizierbar, weil ein Dritter – etwa die Staatsanwaltschaft – diese Zusammenführung bei sich vornehmen kann. Gleich, ob eine Strafanzeige bzw. Einschaltung anderer Behörden erfolgt; gleich, ob die Staatsanwaltschaft überhaupt den Anschlussinhaber ermittelt; gleich, ob – das führt aber der BGH schon gar nicht mehr aus – der Website-Betreiber als Verletzter im Wege der Ausübung eines Akteneinsichtsrechts an die zusammengeführten Daten gelangen kann oder will; gleich, ob dieser Geschehensablauf in kurzer Zeit millionenfach für eine große Anzahl von gespeicherten IP-Adressen möglich oder wirtschaftlich wäre (wenn das massenhaft passieren würde, würden deutsche Staatsanwaltschaften das wohl einen „denial of service"-Angriff auf sich selbst nennen): Alleine die Möglichkeit dieses Geschehensablaufs macht die dynamische IP-Adresse zu einem personenbezogenen Datum. Dies sei, so der EuGH, ein Fall der sogenannten „indirekten Identifikation", damals noch nach der Vorläuferregelung der DSGVO, der EU-Datenschutzrichtlinie. Es sei nicht erforderlich, dass „sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen

einer einzigen Person befinden“. Seither ist in „ähnlichen“ Fallkonstellationen das große Rätseln angesagt, ob eine Person identifizierbar ist oder nicht, sprich, ob die Entscheidung des EuGH übertragen werden kann. Vertieft wird dieses Thema im Kontext der Anonymisierung von Daten unten in Fall 32. Wohlgemerkt: Es geht hier nicht um eine Detailentscheidung in der siebten Verästelung einer DSGVO-Pflicht, sondern darum, ob überhaupt personenbezogene Daten vorliegen, mit anderen Worten, ob das Datenschutzrecht auf bestimmte Informationen Anwendung findet oder nicht.

Auch wenn vor Erlass der genannten Entscheidungen viele Aufsätze publiziert wurden und verschiedene Gerichte bereits unterschiedliche Entscheidungen zu dieser Frage gefällt hatten – auch das Landgericht Berlin war im konkreten Fall als Vorinstanz noch anderer Ansicht gewesen –, war das später vom EuGH (und nachfolgend wieder vom BGH) gefundene Ergebnis nicht vorhersagbar gewesen. Nun sind die Würfel „irgendwie“ gefallen. Diese Rechtsunsicherheit hätte natürlich einfach verhindert werden können, wenn der Datenschutz-Gesetzgeber sich bemüßigt gesehen hätte, im Gesetzes- bzw. Verordnungstext sinngemäß, aber unmissverständlich zu regeln, dass eine dynamisch vergebene IP-Adresse ein personenbezogenes Datum darstellt. Oder ein Grundstückswert, weil sich hieraus die Grundsteuer, die der Eigentümer jährlich zahlen muss, errechnen lässt. Aber so etwas schickt sich für den Gesetzgeber nicht. Er schreibt lieber weiter kryptische Sätze wie „*Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten*“. Man kann das für die Krone der Gesetzgeberschöpfung halten oder für den Auslöser dafür, dass viele Rechtsanwender – man denke an ein typisches mittelständisches Unternehmen – den Kopf in den Sand stecken und denken: Bevor ich es aufwendig, aber sowieso falsch mache, mache ich es lieber gar nicht.

Man könnte dieselbe Geschichte über das EuGH-Urteil vom Juni 2018 zum Thema Verantwortlichkeit für Facebook-Fanpages erzählen. Letztlich ging es dort darum – aber das ist unter einem Berg von Kompetenz- und Prozessthemen fast untergegangen –, dass die Benutzer der Facebook-Fanpage weder von Facebook noch vom Betreiber der Facebook-Fanpage darauf hingewiesen wurden, dass ein session- (und seiten-) übergreifender Zwei-Jahres-Cookie mit einer den Benutzer identifizierenden Kennung verwendet wurde. Damit wurde der Benutzer in einem letztlich immer noch unbekannten Maße „getrackt“ (manchmal will man ja auch gar nicht wissen, was mit den Daten in den USA „wirklich“ passiert). Von dort aus

entspann sich die Frage, ob nun nur Facebook oder auch der Fanpage-Betreiber für diesen Mangel an Aufklärung oder – alternativ – für dieses „Zuviel" an Verarbeitung verantwortlich ist. Der EuGH hat sinngemäß entschieden, dass bei jeder Form des gemeinsamen Anbietens von Datenverarbeitungstätigkeiten sämtliche „Player" datenschutzrechtlich haften. Ob der Fanpage-Betreiber wusste, wie bzw. mit welchen Mitteln Facebook welche Daten überhaupt generiert – bei ihm selbst kam vergleichsweise wenig davon an, und auch dies nur in anonymer Form –, spielte dabei keine Rolle. Mitgefangen, mitgehangen. Auch dieses Thema wurde im Vorfeld kontrovers diskutiert und schon anhand der unterschiedlichen Entscheidungen der involvierten Gerichtsinstanzen wird deutlich, dass die Würfel zwar geworfen, aber noch lange nicht gefallen waren.

Die vorstehend angerissenen Fragen zur Unbestimmtheit des DSGVO-Texts, zur Unvorhersehbarkeit der juristisch bindenden Interpretation und zur thematischen „Breitenwirkung" der DSGVO geben einen Fingerzeig in Richtung der rechtstheoretischen und rechtsphilosophischen Probleme moderner Gesetzgebung bzw. Gesetzgebungstechnik. Diese Fragen werden am Ende des White Papers in einem Exkurs noch weiter vertieft, denn es lohnt sich für jeden Interessierten – ob Jurist oder Nichtjurist –, auch einmal generell darüber nachzudenken, ob und warum Gesetze gut „funktionieren" oder nicht.

➢ Zur Sache!

Den Hauptteil dieses White Papers bildet aber nachfolgend die Darstellung einiger ausgewählter Problembereiche bei der Anwendung der DSGVO auf konkrete Sachverhalte, die sich in der praktischen Arbeit mit dem Gesetzestext im Unternehmensumfeld ergeben haben. Die Aufstellung folgt keiner besonderen Ordnung und hat selbstverständlich auch keinen Anspruch auf Vollständigkeit. Soweit die dabei auftretenden Probleme in der „juristischen Öffentlichkeit" (von den Gerichten, den Aufsichtsbehörden, der Kommentarliteratur etc.) thematisiert werden, zeigt sich häufig das übliche Bild: Jede denkbare Meinung wird vertreten. Erhellende Rechtsprechung gibt es bislang kaum und auch der Hinweis auf die vormalige (seltene) Rechtsprechung zum alten Bundesdatenschutzgesetz und der seit 1995 dahinterstehenden EU-Datenschutzrichtlinie, dem Vorläufer der DSGVO, kann richtig sein oder auch nicht. Im Gegenteil: Wie immer – aber das nehmen Juristen gar nicht mehr als solches wahr, weil die sich für sie ergebenden „Argumentationsspielwiesen" ja ihr täglich Brot sind – werfen die „punktuellen Brösel" höchstrichterlicher Rechtsprechung mehr Probleme bei der juristischen Extrapolation auf ähnliche Fälle bzw. benachbarte Fallgruppen auf, als sie im konkret entschiedenen Fall lösen. Wer in den Krümeln sucht, wer aus dem Kaffeesatz liest, der findet. Die Historie der Kommentierungen zu den einzelnen nachfolgenden Fällen zeigt gut, dass die punktuellen Gerichtsentscheidungen wie auch die punktuellen

Aussagen der Aufsichtsbehörden in ihren Veröffentlichungen das Gesamtbild immer komplexer – und teils widersprüchlicher – machen. Fälle, die ursprünglich auf wenigen Seiten kommentiert werden konnten, nehmen nun mit ihren „Girlanden“ und argumentativen Verästelungen immer breiteren Raum ein.

Man darf in diesem Zusammenhang auch nicht vergessen, dass ein Berater grundsätzlich den „sichersten Weg“ zu empfehlen hat. Welche Empfehlungen vor diesem Hintergrund in den nachfolgenden Fällen deshalb zu geben sind, und dass diese Empfehlungen dem leicht dahingesagten Ausspruch des „gesunden Menschenverstandes“, der angeblich der beste Ratgeber bei der Umsetzung der DSGVO ist, oft zuwiderlaufen dürften, kann sich jeder leicht ausmalen. Im obigen Beispiel der dynamischen IP-Adresse beispielsweise dürfte das Fazit lauten: Man kann letztlich bei keinem relevanten Datum ausschließen, dass es nicht doch irgendeinen Personenbezug aufweist. Einfacher wird die Handhabung der DSGVO durch die Gratwanderung zwischen sicherstem Weg und dem „Augenmaß“, welches mittelständische Unternehmen in der Praxis vom Berater einfordern, sicher nicht.

Fall 1:
Stellt das „Übermittelterhalten“ von personenbezogenen Daten ein „Erheben“ dar?

Praktischer Fall: Herr Müller, Einkäufer der Huber AG, übergibt einem Vertriebsmitarbeiter der Maier GmbH, Herrn Schulze, eine Visitenkarte von sich mit den Worten „Wenn Sie mal das Produkt X in Richtung Y weiterentwickeln, dann rufen Sie mich an“.

Unternehmensbezogene Kontaktdaten von Mitarbeitern (Name, betriebliche Telefon- und Mobilfunknummer, betriebliche E-Mail-Adresse etc.) sind zwar mutmaßlich „Niedrigrisikodaten“, aber diese Erkenntnis kann allenfalls das Maß der notwendigen technisch-organisatorischen Maßnahmen bei deren Verarbeitung reduzieren. Ansonsten – etwa bei den Fragen der Pflichthinweise, der Legitimationsgrundlage oder der Löschfristen – sieht die DSGVO keinerlei Ausnahmen oder Erleichterungen für diese Datenkategorien vor.

- Erhebung von Daten

Man kann diesen Fall nun so interpretieren, dass die Maier GmbH als Verantwortliche im Sinne der DSGVO durch ihren Repräsentanten, Herrn Schulze, personenbezogene Daten von Herrn Müller „erhebt“. Dass die DSGVO anwendbar ist, kann kaum bezweifelt werden. Zwar ist die Visitenkarte zunächst noch nicht Gegenstand einer „ganz oder teilweise automatisierten Verarbeitung personenbezogener Daten“. Das wird erst der Fall sein, wenn die Daten in ein CRM- oder sonstiges EDV-System eingegeben werden. Aber üblicherweise stellen Visitenkarten auf Empfängerseite zumindest erst einmal „für die nichtautomatisierte Verarbeitung personenbezogene Daten, die in einem Dateisystem [...] gespeichert werden sollen“ dar. Kaum jemand wird Visitenkarten, denen er irgendeinen Wert beimisst und die er bei Gelegenheit wiederfinden will, einfach nur irgendwo hinwerfen. Die Maier GmbH, vertreten durch Herrn Schulze, müsste Herrn Müller also Pflichthinweise nach Art. 13 DSGVO erteilen, dass sie die Maier GmbH ist, wie ihr Datenschutzbeauftragter erreicht werden kann, zu welchem Zweck die Daten erhoben werden, wann sie gelöscht werden, ob diese gegebenenfalls in einem CRM-System in der Cloud auf US-Servern gespeichert werden und einiges mehr. Herr Schulze müsste Herrn Maier also umgehend Pflichthinweise in die Hand drücken, die eigentlich auch auf den Einzelfall der konkret erhobenen Daten zugeschnitten sein müssten. Ob diese Hinweise auch nur aus einem Link auf eine Website bestehen können, ist eine Frage des dann vorliegenden „Medienbruchs“, die unten in Fall 29 noch behandelt wird. Den Empfang dieser Pflichthinweise müsste sich Herr Schulze quittieren las-

sen, sonst kann er später seiner datenschutzrechtlichen „Rechenschaftspflicht“ nicht nachkommen, nach der er nachweisen können muss, zu jeder Zeit die DSGVO eingehalten zu haben. Herr Maier könnte ja später behaupten, die Pflichthinweise nie erhalten zu haben.

- Zugang der Pflichtinformationen

Schon an dieser Stelle würden Datenschutzbehörden natürlich einhaken, dass kein Betroffener verpflichtet ist, den Empfang von Pflichthinweisen zu bestätigen. Der Thüringer Landesbeauftragte für Datenschutz schreibt hierzu in seinem Tätigkeitsbericht 2018:

„Art. 5 Abs. 2 DS-GVO schreibt nicht vor, in welcher Form der Nachweis erfüllt werden muss. Eine Gegenzeichnung ist somit nicht zwingend. Es sollte jedoch zumindest eine (schriftliche) Dokumentation erfolgen, aus der zu Nachweiszwecken hervorgeht, dass die Informationspflichten erfüllt wurden.“

Und an anderer Stelle:

„Das Gesetz sieht nicht vor, dass die Erteilung der Information von betroffenen Personen bestätigt werden müsste. Die betroffene Person muss die Möglichkeit haben, diese Informationen zur Kenntnis zu nehmen und danach umfassend ihre Betroffenenrechte ausüben zu können. Es ist daher ausreichend, wenn Unternehmen oder sonstige nicht-öffentliche Stellen ein Verfahren in ihren Geschäftsablauf integriert haben, das sicherstellt, dass die betroffenen Personen zu den in der DS-GVO geforderten Zeitpunkten diese Informationen erhalten. Sofern beispielsweise beim ersten Betreten des Geschäfts die Informationen an die Kunden ausgehändigt werden (mittels Flyer, Informationsbroschüre oder Informationsblatt) oder auf den entsprechenden Aushang verwiesen wird, reicht diese Vorgehensweise als Nachweis für die Erfüllung der Informationspflicht gegenüber den betroffenen Personen aus.“

Auch der Hessische Beauftragte für Datenschutz sieht dies in seinem Tätigkeitsbericht 2018 ähnlich, zählt aber die Erfüllung der Informationspflichten von vornherein nicht zu den nachzuweisenden Pflichten des Verantwortlichen:

„Die Pflicht des Verantwortlichen, den Betroffenen über die Datenverarbeitung zu informieren, führt nicht zu einer Verpflichtung des Betroffenen, den Erhalt der Information durch Unterschrift zu quittieren. [...] M.E. fällt die Informationspflicht nach Art. 13/Art. 14 DS-GVO nicht unter die nach Art. 5 Abs. 1 DS-GVO nachzuweisenden Pflichten des Verantwortlichen.“

Reicht es also, wenn Herr Maier später (etwa gegenüber einer Datenschutzaufsichtsbehörde oder vor Gericht) behauptet, die Pflichthinweise nie erhalten zu haben, die Vorlage einer schriftlichen Anweisung an Herrn Schulze aus, dass dieser jedem, dem er seine Visitenkarte überlässt, auch die Pflichthinweise übergeben muss? Wenn dies ausreichend wäre, müsste es Herr Schulze ja mit dieser unternehmensinternen Vorgabe einfach nur „nicht so genau nehmen". Oder muss die Einhaltung kontrolliert werden? Und wenn ja, wie?

Wer sich übrigens fragt, ob es ausreicht, auf einer Pflichtinformation, die auf ein Erheben von Visitenkartendaten abstellt, keine Bezeichnung der erhobenen Daten zu nennen (das sieht Art. 13 DGSVO nämlich auch gar nicht explizit vor) oder einfach „Visitenkarteninhalte" aufzuführen, wird ebenso im Tätigkeitsbericht 2018 des Thüringer Landesbeauftragten für Datenschutz fündig:

„Dabei ist zu berücksichtigen, dass für jeden Verarbeitungszweck die entsprechend verarbeiteten Daten detailliert und exakt genannt werden (z. B. Telefonnummer, Geburtsdatum, EMail-Adresse usw.). Allein die Angabe von Datenkategorien zum Zweck der Verarbeitung ist zu allgemein gehalten und entspricht nicht den Vorgaben der DS-GVO."

In den Pflichtinformationen des Erhebenden sind also die auf der Visitenkarte angegebenen (erhobenen) Daten eigentlich genau zu bezeichnen.

➢ Übermittlung von Daten

Man kann den Ausgangsfall aber auch so interpretieren, dass die Huber AG, vertreten durch Herrn Müller, der Maier GmbH, vertreten durch Herrn Schulze, die Kontaktdaten ihres zuständigen Ansprechpartners, Herrn Müller, „übermittelt". Bei dieser Mitteilung könnte ja alternativ auch Frau Schmidt von der Huber AG die Kontaktdaten ihres Kollegen Herrn Müller „übermitteln" – dann fallen die Person des (für die Huber AG) Übermittelnden und der eigentlich benannte Ansprechpartner auseinander und der Fall wird noch deutlicher.

Bei dieser Interpretation stellt sich nun die entscheidende Frage, ob das „Übermittelterhalten" dieser personenbezogenen Daten dem „Erheben" gleichgestellt ist, ob also der Übermittlungsempfänger ebenso verfahren muss wie oben dargestellt. Wenn das so wäre, gäbe es viel zu tun: Pausenlos übermitteln Unternehmen und Behörden personenbezogene Daten untereinander. Alleine für jeden Arbeitnehmer sind vom Arbeitgeber regelmäßig und anlassbezogen Meldungen abzusetzen an Finanzämter, Versicherungsträger und andere Institutionen. Ständig benennen Unternehmen ihre Mitarbeiter gegenüber anderen Unternehmen oder Institutionen als Ansprechpartner für dieses und jenes. Regelmäßig wird in solchen Fällen

die betroffene Person nicht vom Übermittlungsempfänger separat informiert, obwohl dies in jedem Fall spätestens einen Monat nach der Erhebung geschehen müsste (Art. 14 Abs. 3 lit. a DSGVO). Sollen all diese Informationsaustausche im Rahmen dieses ständigen Datenverkehrs, weil ständig auf der Empfängerseite Daten „erhoben" werden, künftig zu einer Benachrichtigungsflut beim Betroffenen anschwellen? Der Gesetzgeber würde wohl auf andere Fallkonstellationen bei der Übermittlung verweisen, beispielsweise, wenn Facebook die Daten eines Kunden an Cambridge Analytica „übermittelt" und es dann doch besser wäre, wenn der Betroffene davon erfahren würde, oder auf den Fall des stillen Factorings und der Datenübermittlung an den Forderungskäufer (s. dazu u. Fall 14).

➢ Inhalt der Pflichtinformation

In diesem Zusammenhang muss sich der Verantwortliche beim Design der Pflichtinformationen entscheiden, ob er nun von einem Fall des Art. 13 oder des Art. 14 ausgeht, wenn man einen Bescheid der österreichischen Datenschutzbehörde vom November 2018 liest:

„In der erteilten Information wird strukturell nicht unterschieden, ob diese nach Art. 13 oder Art. 14 DSGVO erteilt wird. Diese Unterscheidung ist jedoch insofern von Bedeutung, als nach Art. 14 DSGVO auch Informationen zu erteilen sind, die Art. 13 DSGVO nicht abdeckt. So ist etwa nach Art. 14 Abs. 1 lit. d die Information zu erteilen, welche Kategorien personenbezogener Daten verarbeitet werden; ebenso ist – anders als in Art. 13 – auch die Information über die Herkunft der Daten zu erteilen (Art. 14 Abs. 2 lit. f DSGVO). [...] Indem in den Informationspflichten nicht klar zwischen den Informationspflichten nach Art. 13 und Art. 14 DSGVO unterschieden wird, hat die Verantwortliche gegen diese Pflichten sowie Art. 12 Abs. 1 DSGVO verstoßen."

Damit nicht genug: Eine weitere Entscheidung der österreichischen Datenschutzbehörde vom November 2018 zu einer unterlassenen Pflichtinformation nach Art. 14 DSGVO sowie zu inhaltlich unrichtigen Daten könnte nahelegen, dass – zumindest in Bezug auf die Legitimationsgrundlage der Interessenabwägung, die im Falle der Erhebung im Sinne von Art. 14 DSGVO aber den Regelfall darstellt – ohne Pflichtinformation das legitimierende Interesse des Verantwortlichen „nicht mehr gerechtfertigt" ist und damit die Verarbeitung rechtswidrig ist bzw. wird. Es geht also nicht nur um den Verstoß gegen die Informationspflichten, sondern im Grunde auch um „toxische" Daten an sich, die nicht mehr weiter verarbeitet werden dürfen. Diese Frage stellte sich schon Europäische Gerichtshof in einem Urteil vom Oktober 2015 zur damaligen EU-Datenschutzrichtlinie, als er – vereinfacht ausgedrückt – feststellte, dass Daten nicht (durch staatliche Stellen an andere staatliche Stellen) übermittelt werden

dürfen, wenn dem Betroffenen die Pflichtinformationen nicht erteilt wurden. Seither wird über die Reichweite dieser Entscheidung gerätselt (s. dazu auch noch unten Fall 26).

➢ Pflichten des Übermittelnden und des Übermittlungsempfängers

Selbst wenn ein „Übermittelterhalten" von personenbezogenen Daten aber nun gar keine Pflichthinweise notwendig machen würde, weil es kein „Erheben" ist, bleibt dennoch die Frage, welche Pflichten der Übermittelnde in Bezug auf die weitere Verwendung und der Übermittlungsempfänger in Bezug auf die Herkunft der Daten hat. Müsste die Huber AG der Maier GmbH zusätzlich zu den personenbezogenen Daten von Herrn Müller selbst nicht auch die Informationen über die Bedingungen der weiteren Verarbeitung mit auf den Weg geben? Schließlich betreffen die Daten nicht die Huber AG, sondern Herrn Müller. Und müsste die Maier GmbH sich nicht von der Huber AG zusichern lassen, dass die Huber AG die Daten rechtmäßig bei Herrn Müller erhoben hat? Schließlich kann die Maier GmbH nicht sicher wissen, ob dies der Fall ist, also beispielsweise, ob eine von Herrn Müller gegebene Einwilligung in den Druck „seiner" Visitenkarten im datenschutzrechtlich-arbeitsrechtlichen Sinne „freiwillig" war. Dieses Thema wird unten in Fall 12 noch weiter erörtert.

Doch damit nicht genug. Die Huber AG müsste sich zusätzlich überlegen, ob sie Herrn Müller die Übermittlung vorab mitteilen muss. Der Thüringer Landesbeauftragte für Datenschutz schreibt in seinem Tätigkeitsbericht 2018 unter Anspielung auf die (erneuten) Pflichtinformationen bei einer Zweckänderung:

„Eine Übermittlung an einen Dritten ist häufig auch eine Zweckänderung, sodass schon aus diesem Grund vor der Übermittlung die betroffene Person erneut zu informieren ist."

Diese Passage wirft im vorliegenden Fall – ungeachtet der Pflichtinformationen – die Frage auf, ob die Übermittlung von unternehmensbezogenen Kontaktdaten eines Mitarbeiters an einen Dritten eine Zweckänderung sein kann. Die unternehmensbezogenen Kontaktdaten werden vom Verantwortlichen (Arbeitgeber) zu Zwecken der Durchführung des Beschäftigungsverhältnisses – also zu vertraglichen Zwecken – generiert. Umfasst dieser (anstellungs-) vertragliche Zweck auch die Übermittlung der unternehmensbezogenen Kontaktdaten an Dritte? Diese Frage (s. im Hinblick auf die „Personalaktendaten" des Beschäftigten auch unten Fall 7 sowie zu den „Bewegungsdaten" des Beschäftigten unten Fall 4) ist nicht so akademisch, wie es scheint. Stützt sich die Übermittlung auf das Anstellungsverhältnis als datenschutzrechtliche Legitimationsgrundlage, könnte sich vielleicht auch der Empfänger – die Maier GmbH – darauf berufen: Die Verarbeitung bei der Maier GmbH ist *„für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, erforderlich"*. Dass dieser

Vertrag mit der Huber AG besteht, schließt ja nicht aus, dass die Verarbeitung der unternehmensbezogenen Kontaktdaten durch die Maier GmbH erforderlich ist, wenn und solange Herr Müller Einkäufer der Huber AG mit Außenwirkung ist und die Maier GmbH mit diesem „Exponenten" der Huber AG unternehmensbezogen kommuniziert. Geht man nicht hiervon aus, kann sich die Maier GmbH nur auf eine Einwilligung (dazu unten Fall 8) oder auf eine Interessenabwägung stützen. Wenn Herr Müller zu einem Zeitpunkt, zu dem er noch Mitarbeiter der Huber AG ist, von der Maier GmbH die Löschung seiner Visitenkartendaten verlangt, ist die Frage, ob er widerrufs- oder widerspruchsberechtigt ist oder nicht, aber ganz wesentlich.

➢ Erheben oder Übermitteln?

Art. 13 und 14 DSGVO sprechen vom „Erheben", nicht vom „Empfang". Nach Art. 4 Nr. 9 DSGVO ist „Empfänger" eine Stelle, „der personenbezogene Daten offengelegt werden". Ist „Erheben" nun etwas anderes als „offengelegt-bekommen"? Und warum wird punktgenau nur in Art. 14 Abs. 4 DSGVO statt dem Begriff „übermittelt" der allgemeinere Begriff „erlangt" verwendet, der in der DSGVO nicht definiert wird, während in der englischen Sprachfassung der DSGVO die Begriffe „collect" und „obtain" in Art. 13 Abs. 1 und 14 Abs. 1 und 4 wild durcheinander verwendet werden? Diese Thematik wird in der juristischen Kommentarliteratur nicht vertieft behandelt. Teils wird in Bezug auf Beispielsfälle kurz festgestellt, dass Daten übermittelt und damit gerade nicht „erhoben" wurden (sodass der Empfänger auch keine Pflichthinweise erteilen musste, vgl. auch den Fall der Übermittlung einer Traueranzeige in Fall 14 unten). Teils wird ohne weitere Begründung behauptet, dass „der Empfänger übermittelter Daten diese Daten erhebt, indem er sie zielgerichtet entgegennimmt, um sie weiterzuverarbeiten". Das bereits oben erwähnte EuGH-Urteil vom Oktober 2015 postuliert in der Tat, es sei sogar „Voraussetzung" für die Verarbeitung „übermittelter" Daten, dass der Übermittlungsempfänger dem Betroffenen die Pflichthinweise mitteilt. Auch die Berliner Datenschutzbeauftragte ist explizit der Ansicht, dass der Käufer einer Forderung, der die Daten des Schuldners erhält, diesem Pflichtinformationen nach Art. 14 DSGVO zu erteilen hat (s. dazu noch unten Fall 14). Nimmt man die oben erwähnte Auffassung des Thüringer Datenschutzbeauftragten hinzu, müssten also die meisten Betroffenen zwei Pflichtinformationen erhalten, eine vom Absender (Zweckänderung) und eine vom Empfänger (Erheben).

Es wäre in jedem Fall wünschenswert gewesen, dies im Gesetz klarzustellen, denn die „Breitenwirkung" dieses Postulats (das kaum jemand in der Praxis befolgt) ist enorm und die spezifische Aussage des EuGH wurde in der Zwischenzeit kaum rezipiert. Der Begriff der Übermittlung wird zwar in der DSGVO genannt, aber nicht definiert: In Art. 4 Nr. 2 DSGVO wird

die Übermittlung als ein Fall der Offenlegung bezeichnet und danach wird der Begriff – abgesehen von der Verwendung im Zusammenhang mit dem Recht des Betroffenen auf Datenübertragbarkeit (Art. 20 DSGVO) – ausschließlich im Kapitel über die Übermittlung personenbezogener Daten an Drittländer (Art. 44 bis 50 DSGVO) verwendet. Es hätte daher nahegelegen, das Pendant der Übermittlung auf Empfängerseite, das „Übermittelterhalten", zu definieren und dann klar in Art. 14 DSGVO zu regeln, ob dem Betroffenen die Pflichthinweise (vorbehaltlich der ausdrücklich geregelten Ausnahmen) bei jedem „Übermittelterhalten" aufseiten eines Übermittlungsempfängers mitzuteilen sind.

Im Zusammenhang mit der Auftragsverarbeitung schreibt der Thüringer Landesbeauftragte für Datenschutz in seinem Tätigkeitsbericht 2018:

„Zudem sind Auftragsverarbeiter Empfänger im Sinne des Art. 4 Nr. 9 der DS-GVO von personenbezogenen Daten. Das führt dazu, dass der Verantwortliche im Rahmen seiner Informationspflichten nach Art. 13 und 14 der DS-GVO den Auftragsverarbeiter als Empfänger zu benennen hat."

Bedeutet dies dann, dass der Auftragsverarbeiter als Übermittlungsempfänger auch „erhebt" und dann dem Betroffenen Pflichtinformationen über die zur Auftragsverarbeitung empfangenen Daten zukommen lassen muss?

Auch die „Orientierungshilfe" der Datenschutzkonferenz zum Thema Direktwerbung vom November 2018 beschäftigt sich nicht mit der Differenzierung zwischen „Erheben" und „Übermittelterhalten". Zwar wird dort der Fall der Übergabe einer Visitenkarte durch eine betroffene Person mit dem Ziel der „weiteren geschäftlichen Kontaktaufnahme" behandelt, dabei aber nicht berücksichtigt, dass der Betroffene in dieser Konstellation durchaus (bzw. sogar im Regelfall) als Emissär eines Unternehmens mit Wirkung für dieses Unternehmen auftritt und die Visitenkarteninhalte auch für dieses Unternehmen (im datenschutzrechtlichen Sinne) „übermitteln" könnte. Wie oben angedeutet, könnte die Person ja auch die Visitenkarte bzw. Kontaktdaten eines Kollegen desselben Unternehmens übergeben, der z. B. für das in Rede stehende Thema der bessere Ansprechpartner ist (oder eine entsprechende E-Mail schicken). Allerdings enthält die „Orientierungshilfe" den lapidaren Satz:

„Sollen personenbezogene Daten der betroffenen Person für Zwecke der Direktwerbung verarbeitet werden, die nicht von dieser Person selbst erhoben wurden, sind die Informationspflichten nach Art. 14 Abs. 1 und 2 DSGVO zu beachten".

Man kann dies so lesen, dass nur der Gesetzestext des Art. 14 DSGVO (wenn auch etwas undeutlich) wiedergegeben wird: Werden die Daten des Betroffenen erhoben, aber nicht „bei der betroffenen Person", wie es in Art. 14 DSGVO heißt, dann gilt natürlich Art. 14 DSGVO. Man könnte es aber auch so lesen, dass – ohne weitere Begründung – die Datenschutzbehörden nun jedes Übermittelterhalten als „Erhebung" ansehen. Deutlich wird dies nicht. Man darf gespannt sein, wie in einigen Jahren die Würfel fallen, die die DSGVO in die Höhe geworfen hat.

➢ Parallelfall: Webseite

Viele Sachverhalte im Umgang mit digitalen Daten machen das Problem im Umgang mit dem Begriff des „Erhebens" deutlich. Schreibt eine Privatperson an ein Unternehmen, es möge ihr dessen aktuellen Katalog an die angegebene Adresse der Privatperson schicken, wird jeder Datenschutzrechtler davon ausgehen, dass die Adresse „erhoben" wurde. Dabei ist irrelevant, wie lange diese Adresse vom Unternehmen „gespeichert" wird. Wie sieht es aber mit dem einfachsten möglichen digitalen Pendant aus – also bei „granularer Sichtweise" (dazu u. Fall 14)? Der Browser einer surfenden Privatperson sendet eine HTTP-Anfrage an den Server des Unternehmens, es möge ihm dessen aktuelle Webseite an die angegebene Ziel-IP des Rechners, vor dem die surfende Privatperson gerade sitzt, schicken. Ist das nicht ebenso eine Erhebung, gleich, wie lange diese IP-Adresse vom Server des Unternehmens gespeichert wird? Typologisch gibt es eigentlich keinen Unterschied, den müsste man mühsam konstruieren. Muss dies nun dazu führen, dass eine Datenschutzerklärung des Inhalts „Wir erheben auf dieser Webseite keine personenbezogenen Daten" falsch ist, und dass eine Datenschutzerklärung, die hinsichtlich der Speicherung von IP-Adressen nur auf Server-Logfiles und die „mittelfristige" Speicherung der IPs zu Zwecken der Aufrechterhaltung des Webseiten-Dienstes Bezug nimmt, unvollständig ist? Man weiß es nicht.

➢ Parallelfall: Paketdienst

Ein anderes Beispiel: Auf der Website eines Paketdienstes – als selbstständig Verantwortlichem – werden (vom Absender) die Daten des Empfängers eines Pakets eingegeben und daraus das Sendungsetikett erzeugt, das auf das Paket geklebt wird. Werden die Empfängerdaten dem Paketdienst „übermittelt" oder „erhebt" der Paketdienst die Daten des Empfängers? Wenn man hier von einer „Erhebung" ausgehen würde, wäre Art. 14 DSGVO einschlägig – dem Empfänger müssten die Pflichtinformationen vom Paketdienst mitgeteilt werden. Dies geschieht aber gewöhnlich weder bei der Eingabe der Empfängerdaten noch bei der Inempfangnahme des Pakets noch bei dessen Auslieferung. Dabei muss man noch gar nicht

an die (tatsächliche) Erhebung der Daten der dritten Person denken, bei der ersatzweise zugestellt wird (Nachbar, Mitbewohner) und die dem Mitarbeiter des Paketdienstes Name und Unterschrift hinterlässt. Dass die polnische Datenschutzbehörde in einem Fall, der – um es vorsichtig auszudrücken – möglicherweise strukturell vergleichbar ist, die Versendung von E-Mails und Briefen mit Pflichtinformationen an die Betroffenen für verhältnismäßig bzw. zumutbar gehalten hat, wird unten in Fall 22 aufgezeigt.

Das Gleiche gilt für die (vielen) Fälle, in denen Einzelhändler für mit Endkunden vereinbarte Direktlieferungen die Endkundenadressen an Hersteller oder Großhändler weitergeben (beauftragte Warenzusendung) – übrigens auch hier nach der „Auslegungshilfe" des Bayerischen Landesamts für Datenschutzaufsicht zur Frage *„Was ist Auftragsverarbeitung und was nicht?"* kein Fall der Auftragsverarbeitung, sondern ein Fall zweier selbstständiger Verantwortlicher (weil bei der Dienstleistung Kommissionierung und Versand nicht die Datenverarbeitung im Vordergrund steht, s. unten Fall 7).

- Drittländer

Es geht aber noch weiter: Wenn Klaus Schmidt in Google den Suchbegriff „Franz Lehmann" eingibt, dann „weiß" Google (USA) von Klaus Schmidt – identifiziert anhand von dessen Google-Konto, zumindest aber von dessen IP-Adresse –, dass er Informationen zu Franz Lehmann sucht und (durch Klicken auf Links bzw. Suchergebnisse) erhebt. Die Erhebung personenbezogener Daten von Franz Lehmann durch Klaus Schmidt stellt also gleichzeitig auch eine Übermittlung personenbezogener Daten von Klaus Schmidt sowie von Franz Lehmann (nämlich, dass Klaus Schmidt bestimmte Informationen über Franz Lehmann sucht) an Google (USA) dar. Unabhängig von der Frage, ob und wann Klaus Schmidt als erhebender und übermittelnder Verantwortlicher Franz Lehmann hierüber Pflichthinweise zur Verfügung stellen muss – Klaus Schmidt ist schließlich auch als Privatperson insoweit „Verantwortlicher" (s. dazu u. Fall 18) –, müsste Google (USA) als Übermittlungsempfänger Franz Lehmann über diese Übermittlung mit Pflichthinweisen informieren. Das setzt lediglich voraus, dass Franz Lehmann eine für Google (USA) mit zumutbaren Mitteln identifizierbare Person ist. Wir erinnern uns (s. Einleitung), dass Erwägungsgrund 26 der DSGVO vorgibt, dass dabei *„alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren"*. Und wer hat nicht schon mal jemanden „gegoogelt"?

➢ Erheben oder Hergeben?

In einer Entscheidung des Bundesgerichtshofs zum Thema „Zugriff der Erben auf den Facebook-Account des Erblassers“ vom Juli 2018 findet sich übrigens ein interessanter Satz zu dem Thema, zu dem nun wieder gerätselt werden darf, ob er „nur so dahingesagt“ wurde oder ein ganz anderes Begriffsverständnis des BGH zeigt. Bei Nachrichten, die A an B über Facebook schreibt – sowohl A als auch B sind Facebook-Teilnehmer und damit Vertragspartner von Facebook –, handele es sich nicht um von Facebook „erhobene, sondern um von den Kommunikationspartnern im Rahmen des bestehenden Vertrags (EG 47 Satz 2) freiwillig und selbstbestimmt sowie inhaltlich kontrollierbar übersandte Daten“. Die Kommentarstelle, auf die der BGH verweist, beschäftigt sich allerdings mit den in eine Interessenabwägung einzustellenden Interessen, nicht mit dem Thema Erhebung. Wenn man den BGH wörtlich nehmen würde, dann wäre (zumindest) überall dort nicht von einem „Erheben“ im datenschutzrechtlichen Sinne auszugehen, wo jemand „einfach so“ Daten hergibt, ohne dass er das muss – bei Bewerbungen, Visitenkartenübergaben, E-Mail-Korrespondenz? Das gilt aber nur, wenn der BGH das Wort „Erheben“ hier im strikten Sinne der DSGVO gemeint hat, was niemand weiß. Es gilt also wie so oft: Fröhlich judizierende Richter und Millionen fragender Gesichter.

➢ Löschen unternehmensbezogener Kontaktdaten

Wenn man Beschäftigtendaten grob in die Kategorien Personalaktendaten (für die Administration des Beschäftigungsverhältnisses), unternehmensbezogene Kontaktdaten (im Ausgangsfall oben behandelt) und laufend generierte „Bewegungsdaten“ (s. u. Fall 4) unterscheidet, stellt sich neben der Frage der Erhebung natürlich auch immer die Frage, wann diese zu löschen sind und wer davon ggf. benachrichtigt werden muss (zur Benachrichtigungspflicht s. u. Fall 22, dort auch zu Mitarbeiterfotos).

Unternehmensbezogene Kontaktdaten, die der Arbeitgeber für seine Arbeitnehmer bei deren Einstellung generiert, sind mit Beendigung des Anstellungsverhältnisses obsolet. Der Zweck des Beschäftigungsverhältnisses kann ihre weitere Verarbeitung nicht rechtfertigen. Diese vermeintlich klare und verständliche Botschaft wirft allerdings Folgefragen größerer Komplexität auf – man muss sich nur vor Augen führen, wo überall unternehmensbezogene Kontaktdaten dieses Mitarbeiters gespeichert sind –, die sich auch bei Bewegungsdaten stellen. Auf diese Thematik wird unten in Fall 33 weiter eingegangen.

➢ Das gute Ende

Wer bis hierher gelesen hat, wird mutmaßlich zustimmen, dass die DSGVO es bei genauer Betrachtung mit der „juristischen Lupe“ schwierig macht, einen einfachen Fall wie die Übergabe einer Visitenkarte einer eindeutigen, mit dem Gesetzestext klar zu vereinbarenden Lösung zuzuführen. Man kann es sich aber auch wesentlich einfacher machen, die DSGVO „einen guten Mann sein lassen“ und mit dem gesunden Menschenverstand argumentieren. So findet sich in der FAQ-Sektion des Bayerischen Landesamts für Datenschutzaufsicht auf die Frage *„Welche Informationspflicht bestehen bei Übergabe einer Visitenkarte?“* die verblüffend einfache Antwort:

„In den meisten Fällen keine, da die Kontaktdaten der Verantwortlichen und der Zweck (Zusendung von Infomaterial) klar sind. Nur wenn ein abweichender Zweck beabsichtigt ist, bestehen weitergehende Informationspflicht.“

Dieses Verständnis beruht auf einem weiten Verständnis von Art. 13 Abs. 4 bzw. Art. 14 Abs. 5 lit. a DSGVO, wonach es keiner Pflichtinformationen bedarf, wenn die betroffene Person „bereits über die Informationen verfügt“. Ob dies nach allem, was sich oben an Problemen im Detail auftürmt, so einfach behauptet werden kann, und ob der Zweck der Übergabe einer Visitenkarte in den meisten Fällen die „Zusendung von Infomaterial“ ist, ist eine andere Frage. In der juristischen Kommentarliteratur wird zu Art. 13 Abs. 4 DSGVO Folgendes ausgeführt:

„Abs. 4 schränkt die dargestellten Informationspflichten auf die Fälle ein, in denen die betroffene Person nicht bereits über die Informationen verfügt. [...] Der Informationsgehalt muss demnach aber in Ausmaß, Genauigkeit und Klarheit denen aus den vorherigen Absätzen entsprechen. Zudem reicht es nicht aus, dass die betroffene Person auf irgendeine Art und Weise Kenntnis über die Informationen erhalten hat bzw. erhalten kann, sondern sie müssen ihr nachweislich zur Verfügung stehen. Das beinhaltet auch, dass diese Informationen im Herrschaftsbereich der betroffenen Person sicher vorhanden sind, weshalb die bloße Möglichkeit, sich diese Informationen zu beschaffen, gerade nicht ausreicht (bspw. bestehende Rechtsvorschriften im Netz). Die Informationspflichten können daher nur dann im Sinne des Abs. 4 ausnahmsweise entfallen, wenn der Verantwortliche und die betroffene Person zum Beispiel in ständigem oder wiederkehrenden geschäftlichen Kontakt stehen.“

Der letzte Satz würde gerade bei einem Erstkontakt mit Übergabe einer Visitenkarte die Anwendbarkeit von Art. 13 Abs. 4 DSGVO ausschließen. Wir werden irgendwann sehen, ob der Europäische Gerichtshof dennoch der „progressiven“ Sichtweise folgt.

Fall 2:
Wie muss ein Verantwortlicher mit besonderen Kategorien personenbezogener Daten von Bewerbern umgehen?

Praktischer Fall: Die Huber AG hat ein „Funktionspostfach" (bewerbung@huber-ag-online.de) für die Zusendung von Bewerbungen eingerichtet, das bei allen Online-Stellenanzeigen genannt wird. In diesem Zusammenhang wird auch auf die Pflichthinweise der Art. 12, 13 DSGVO in der Datenschutzerklärung auf der Website hingewiesen, die die für eingereichte Bewerbungen maßgeblichen Informationshinweise enthalten. Die Datenschutzerklärung nennt als Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten in der Bewerbung die Erforderlichkeit für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses (§ 26 Abs. 1 S. 1 BDSG). Frau Maier sendet der Huber AG eine E-Mail mit ihrer Bewerbung, welche neben einem Foto auch die Angabe enthält, dass Frau Maier zu 60 % schwerbehindert ist.

Hier ist schon unklar, ob es datenschutzrechtlich zulässig ist, sich Bewerbungen über eine E-Mail-Adresse schicken zu lassen. Darum soll es an dieser Stelle aber nicht gehen, sondern erst unten in Fall 8.

Jede Verarbeitung personenbezogener Daten bedarf einer gesetzlichen Legitimationsgrundlage. Ohne „passende" Legitimationsgrundlage ist die Verarbeitung unrechtmäßig. Grundsätzlich ergeben sich die Legitimationsgrundlagen aus den verschiedenen Alternativen des Art. 6 Abs. 1 DSGVO. Die in der unternehmerischen Praxis wichtigsten Legitimationsgrundlagen sind Einwilligung, Vertrag (bzw. Vertragsanbahnung), Einhaltung (insbesondere nationaler) Gesetze, welche die Verarbeitung vorschreiben, und Interessenabwägung. Die im Fall genannte Rechtsgrundlage für das Verarbeiten der eingereichten Bewerbung stammt aus dem Beschäftigtendatenschutz (§ 26 BDSG), wonach gewöhnliche Kategorien personenbezogener Daten von Bewerbern verarbeitet werden dürfen, *„wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses [...] erforderlich ist"*. Diese Legitimationsgrundlage aus dem BDSG knüpft – aus der Perspektive der in Art. 6 DSGVO aufgezählten Kategorien – für bestehende Beschäftigungsverhältnisse an die Legitimationsgrundlage „Vertrag" an, für die Bewerbungsphase an die Vertragsanbahnung. Aber gilt dies auch für besondere Kategorien personenbezogener Daten wie Gesundheitsdaten (Behinderung oder auch ein Bewerbungsfoto, dem man etwas über den Gesundheitszustand des Bewerbers entnehmen kann)?

Für besondere Kategorien personenbezogener Daten stellt Art. 9 DSGVO besondere Voraussetzungen auf. Die Verarbeitung solcher Daten ist nur zulässig, wenn einer der in Art. 9 Abs. 2 DSGVO genannten Fallkonstellationen vorliegt. Dabei stellt sich die Frage, ob das Vorliegen einer der dort genannten Fallkonstellationen eine hinreichende Legitimationsgrundlage darstellt oder ob zusätzlich immer auch eine der „normalen" Legitimationsgrundlagen vorliegen muss (Art. 6 DSGVO, bekanntlich überschrieben mit „Rechtmäßigkeit der Verarbeitung"). Das hat praktische Konsequenzen vor allem bei den Pflichtinformationen (Art. 13/14 DSGVO), in deren Rahmen die Legitimationsgrundlage (richtig und vollständig) genannt werden muss (s. oben Fall 1), und bei den Voraussetzungen für die Einwilligung, d. h. für den im Rahmen von Art. 6 DSGVO anwendbaren Art. 7 DSGVO (s. dazu unten Fall 8). Der Schlüssel zu diesem Problem verbirgt sich in Erwägungsgrund 51, in dem es heißt:

„Zusätzlich zu den speziellen Anforderungen an eine derartige Verarbeitung sollten die allgemeinen Grundsätze und andere Bestimmungen dieser Verordnung, insbesondere hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung, gelten."

Es müssen also sowohl die allgemeinen Voraussetzungen als auch die besonderen Voraussetzungen des Art. 9 Abs. 2 DSGVO vorliegen.

In den Regelungen des Beschäftigungsdatenschutzes ist zwar ausdrücklich vorgesehen, dass vom Arbeitgeber (Verantwortlichen) auch besondere Kategorien personenbezogener Daten verarbeitet werden dürfen, allerdings nur, wenn die Verarbeitung *„zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht [...] erforderlich ist"* (§ 26 Abs. 3 BDSG). Hier fehlt also die Vertragsanbahnungsphase; nur die Durchführung eines bereits abgeschlossenen Beschäftigungsverhältnisses wird genannt. Es ist unklar, ob der deutsche Gesetzgeber überhaupt für die Anbahnungsphase einen Legitimationsgrund zur Verarbeitung besonderer Kategorien personenbezogener Daten hätte schaffen können. Die entsprechende Öffnungsklausel der DSGVO für den nationalen Gesetzgeber (Art. 9 Abs. 2 lit. b DSGVO) verweist auf die Rechte und Pflichten „aus dem Arbeitsrecht". Möglicherweise ist dies auf ein bestehendes Arbeitsverhältnis beschränkt.

Obwohl die Verarbeitung aus der Perspektive des Art. 6 DSGVO auf die Vertragsanbahnung (Art. 6 Abs. 1 S. 1 lit. b DSGVO) gestützt werden kann, muss nun zusätzlich ein besonderer Legitimationsgrund für die Verarbeitung besonderer Kategorien personenbezogener Daten „gesucht" werden (Art. 9 Abs. 2 DSGVO). In diesem Kontext bleibt nur noch die Alternative der Einwilligung übrig, d. h. Frau Maier müsste unmittelbar nach Eingang ihrer Bewerbung

angeschrieben werden, ob sie damit einverstanden ist, dass besondere Kategorien personenbezogener Daten für die Bearbeitung der Bewerbung verarbeitet werden. Eine solche spezifische Einwilligungserklärung kann auch kaum in der Datenschutzerklärung auf der Website der Huber AG enthalten sein oder (stillschweigend) in der Übersendung der Daten selbst liegen, da sie nach Art. 9 Abs. 2 lit. a DSGVO „ausdrücklich" abgegeben werden muss (s. dazu auch u. Fall 8). Die Anforderungen an eine Einwilligung im Rahmen besonderer Kategorien personenbezogener Daten sind also höher als bei „normalen" personenbezogenen Daten. Eine stillschweigende Einwilligung reicht keinesfalls aus.

Eine solche Bewerbung, wenn sie besondere Kategorien personenbezogener Daten enthält, dürfte eigentlich nicht einfach geöffnet werden; im Grunde würde schon das Speichern der eingehenden E-Mail auf den Servern der Huber AG eine Datenverarbeitung ohne Rechtsgrundlage darstellen. Nach „herrschender Meinung" unter den Juristen ist alleine die „Möglichkeit der Kenntnisnahme" bereits ein Erheben von personenbezogenen Daten, d. h. auch bei „aufgedrängten Daten", deren Inhalt man (noch) nicht kennt, liegt beim Speichern schon eine Datenverarbeitung vor, die einer Legitimationsgrundlage bedarf. Man befindet sich also in einem Zirkelschluss und bis zur Erteilung der Einwilligung in einem Zustand erheblicher Rechtsunsicherheit, weil man diese besonderen Kategorien personenbezogener Daten bis zu einer ausdrücklichen Einwilligung eigentlich „nicht haben darf". Dass es Frau Maier seltsam finden wird, aus datenschutzrechtlichen Gründen der Verarbeitung ihrer eigens eingereichten Bewerbung – aus ihrer Sicht „noch einmal" – zustimmen zu müssen, ist nur noch eine Randnotiz.

Anders sieht dies der Thüringische Landesdatenschutzbeauftragte, der in seinem an datenverarbeitende öffentliche Stellen gerichteten Dokument „Hinweise zu den Informationen zur Erhebung von personenbezogenen Daten" zwischen dem Erheben und dem „Aufdrängen" unterscheidet und zumindest das Vorliegen von Informationspflichten nach Art. 13 DSGVO nur bei einem Erheben annimmt:

„Damit die Informationspflichten nach Art. 13 DS-GVO greifen, muss eine Erhebung von Daten vorliegen. Dies ist nicht der Fall, wenn der Verantwortliche die Daten nicht aktiv beschafft, sondern die Daten der öffentlichen Stelle „aufgedrängt" werden, d.h. von der betroffenen Person selbst oder von Dritten ohne Aufforderung geliefert werden. Damit die Informationspflichten nach Art. 13 DS-GVO greifen, muss eine Erhebung von personenbezogenen Daten bei der betroffenen Person vorliegen. Die Erhebung definiert den Beginn der Datenverarbeitung und liegt vor, wenn der Verantwortliche auf die personenbezogenen Daten erstmals zielgerichtet zugreift, um sie in einem Dateisystem zu verarbeiten."

Auch hier darf man sich darüber „freuen“, dass der DSGVO-Text das Thema nicht deutlich adressiert – das „Erheben“ von Daten wird hier nicht genauer definiert – und damit erhebliche Rechtsunsicherheit herrscht, wen der Verantwortliche wann genau und wie zu informieren hat, wenn die entsprechende Information unaufgefordert eingeht.

In der Praxis hilft dies alles nicht weiter, denn um zu wissen, was der Betroffene vom Verantwortlichen will, muss er die Information zur Kenntnis nehmen – wenn auch vielleicht nur, um zu der Erkenntnis zu gelangen, dass er sie nicht hätte zur Kenntnis nehmen müssen.

Im Grunde stellt sich dieses Problem – wenn auch nicht unbedingt vor dem Hintergrund von Art. 9 DSGVO – bei jeder unverlangt zugesandten E-Mail, weil dem Empfänger vorher unbekannt ist, welche personenbezogenen Daten er erhalten wird. Der Frage, ob im Senden einer E-Mail ohne besondere Kategorien personenbezogener Daten stets eine (stillschweigende) Einwilligung der weiteren Verarbeitung aufseiten des empfangenden Verantwortlichen zu sehen ist, geht auch Fall 8 noch nach. Selbst wenn man von einer Einwilligung ausgehen wollte, bleibt natürlich offen, wie weit diese Einwilligung reicht. Ein einfaches Beispiel wäre eine Journalarchivierung aufseiten des empfangenden Verantwortlichen: Sämtliche eingehenden E-Mails werden – aus welchen Gründen auch immer – standardmäßig in ein Archiv geschrieben. Ob die Einwilligung auch diese Vorgehensweise abdecken würde, ist offen.

Geht man hingegen nicht von einer (stillschweigenden) Einwilligung aus, müsste eigentlich für jede eingehende personenbezogene Information – nach deren „Erhebung“ – eine Legitimationsgrundlage „gesucht“ werden. Dies ist auch notwendig, um die dann folgenden Pflichtinformationen richtig ausgestalten (dazu auch schon oben Fall 1 und noch unten Fall 26) und die Löschfrist richtig bemessen zu können (dazu auch unten noch Fall 14). Im Zweifel ist die Legitimationsgrundlage im Kontext von Art. 6 DSGVO eine Interessenabwägung (s. auch unten Fall 8).

Nur zur Vervollständigung: Neben die „normale“ Legitimationsgrundlage (Art. 6 DSGVO) und die zusätzliche Legitimationsgrundlage bei der Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) tritt bei einer Drittlandsübermittlung der Daten noch die „Drittlands-Legitimationsgrundlage“ (Art. 44 ff. DSGVO, s. dazu auch noch unten Fall 10).

Fall 3:
Inwieweit muss die Belehrung eines Mitarbeiters auf seine Position hin individualisiert werden?

Praktischer Fall: Frau Maier (s. oben Fall 2) wird am Ende des Bewerbungsverfahrens von der Huber AG als Lohnbuchhalterin eingestellt. Sie erhält eine Formular-Belehrung, dass sie im Rahmen ihrer Arbeit mit personenbezogenen Daten zu tun haben wird und das Datenschutzrecht einhalten muss.

Die DSGVO enthält – im Unterschied zum früheren BDSG – keine ausdrückliche Verpflichtung des Verantwortlichen, den Arbeitnehmer „auf das Datengeheimnis zu verpflichten". Geregelt ist lediglich eine Verpflichtung „unterstellter Personen", personenbezogene Daten weisungsgemäß zu verarbeiten (Art. 29 DSGVO), sowie die Verpflichtung des Verantwortlichen selbst, sicherzustellen, dass „unterstellte Personen" die Daten nur weisungsgemäß verarbeiten (Art. 32 Abs. 4 DSGVO). Wie dies sichergestellt wird, ist dem Verantwortlichen überlassen. Nur für Auftragsverarbeiter gibt es eine ausdrückliche Regelung, die Mitarbeiter zu verpflichten (Art. 28 Abs. 3 S. 2 lit. b DSGVO).

Verschiedene Juristen sind der Ansicht, der Mitarbeiter soll weiterhin eine Verpflichtungserklärung unterzeichnen. Allerdings ist der „Zwang", als Arbeitnehmer eine Verpflichtungserklärung abgeben zu müssen, die von der DSGVO nicht gefordert wird, arbeitsrechtlich durchaus kritisch zu sehen. Vielmehr dürfte eine Belehrung des Arbeitnehmers sowie die Quittierung des Empfangs der Belehrung ausreichen, aber auch notwendig sein.

Die entscheidende Frage ist jedoch, wie maßgeschneidert diese Belehrung auf die spezifischen Tätigkeiten des jeweiligen Arbeitnehmers zugeschnitten sein muss. Jeder Arbeitnehmer, noch mehr aber jede Abteilung in einem Unternehmen, erfüllt eine andere Funktion, verarbeitet andere Daten zu anderen Zwecken. Muss nun für jede Abteilung, für jeden Arbeitnehmer eine andere Belehrung erfolgen? Wenn ja, was genau muss wie individualisiert werden bzw. gibt es eine Grenze, bis zu der Aufwand betrieben werden muss?

Die Frage ist auch deshalb von Relevanz, weil in vielen mittelständischen Unternehmen keine schriftlichen Prozessbeschreibungen sämtlicher unternehmensinterner Prozesse vorgehalten werden, aus denen sich für jede Position innerhalb des Unternehmens klar und hinreichend detailliert ergibt, welche personenbezogenen Daten im Rahmen der Tätigkeit wie zu verarbeiten sind. Die „Weisungen", von denen in Art. 32 Abs. 4 DSGVO im Rahmen

der „weisungsgemäßen Verarbeitung“ die Rede ist, existieren in der Praxis häufig nur aufgrund mündlicher Anleitung oder „Vormachen“ durch länger beschäftigte Mitarbeiter, lassen sich also im Streitfall auch kaum mehr im Einzelnen nachweisbar klären. Dies gilt sowohl gegenüber dem Mitarbeiter als auch gegenüber einer Aufsichtsbehörde.

Eine „pro forma“-Belehrung zum Datenschutzrecht wird sich in aller Regel in allgemeinen Hinweisen zur Einhaltung des Gesetzes, ggf. in Schulungen erschöpfen, deren Besuch nachvollziehbar und beweisbar ist. Aber inhaltlich gehen die Vorgaben der Art. 29, 32 DSGVO weiter. Der Arbeitgeber ist insbesondere gehalten, datenschutzrechtliche interne „Befugnisse“ insbesondere auf Basis des „need to know“ zu definieren: Welcher Mitarbeiter darf unter welchen Umständen was mit welchen Daten machen bzw. nicht machen? Dies lässt sich nicht über theoretische Erklärungen zu „Legitimationsgrundlagen“ und Betroffenenrechten lösen. Der Mitarbeiter ist keine datenschutzrechtliche Subsumtionsmaschine und beherrscht das Datenschutzrecht nicht besser als sein Arbeitgeber. Die Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO wird daher die Dokumentation von spezifischen Weisungen an die Arbeitnehmer erfordern, mit denen der Arbeitgeber die DSGVO für „sein“ konkretes Unternehmen in konkrete, rollenspezifische und für die Adressaten verständliche Vorgaben „übersetzt“. Allgemeine Ausführungen stellen keine „Weisungen“ dar und auch der Verweis auf tausende Seiten interner (Compliance-)Dokumentation in Großkonzernen (am besten in Englisch), aus denen sich der Neuankömmling dann das für ihn „Richtige“ heraussuchen muss, stellt zumindest nach Meinung der Arbeitsgerichte keine ordnungsgemäße, aufgabenbezogene Anweisung an den Mitarbeiter dar.

Wichtig ist auch, dass die Belehrung des Beschäftigten, die Pflichtinformationen gegenüber dem Beschäftigten und etwaige vom Beschäftigten möglicherweise abzugebende Einwilligungserklärungen nicht miteinander vermischt werden. Der Landesdatenschutzbeauftragte von Mecklenburg-Vorpommern führt in seinem Tätigkeitsbericht 2018 zu einem als „Datenschutzerklärung“ des Arbeitgebers bezeichneten Dokument, das der Beschäftigte zu unterschreiben hatte, aus:

„Vielfach wird diese reine Information mit anderen Klauseln vermischt und unter dem Begriff ‚Datenschutzerklärung‘ den Betroffenen zur Unterschrift vorgelegt. In einem Fall legte der Arbeitgeber seinen Beschäftigten eine solche „Datenschutzerklärung“ vor. Diese enthielt neben den Informationen nach Art. 13 DS-GVO eine Belehrung über die Schweigepflicht, eine Einwilligungsklausel in die Verwendung von Bild- und Tonaufnahmen der Beschäftigten und eine Einwilligungsklausel in die Verarbeitung der Beschäftigtendaten. Ein Petent, der diese „Datenschutzerklärung“ nicht unterschrieben hatte, meldete sich bei uns, da sein

Arbeitgeber seine Gehaltzahlung zurückhielt mit der Begründung, dass er diese nicht leisten könne, weil der Petent die Datenschutzerklärung nicht unterschrieben habe und er ohne Einwilligung die Beschäftigtendaten nicht verarbeiten dürfe.

Nach unserem zunächst telefonischen Kontakt zum Arbeitgeber wurde dem Petenten sein Gehalt gezahlt. Im danach geführten Schriftverkehr wurde die „Datenschutzerklärung" durch den betrieblichen Datenschutzbeauftragten entwirrt und von den falschen Klauseln, den Einwilligungen und Belehrungen getrennt. Es wurde dem Arbeitgeber erklärt, dass er für die Verarbeitung der erforderlichen Beschäftigtendaten keine Einwilligung benötigt, da es hierfür eine Rechtsgrundlage nach Art. 6 Abs. 1 lit. b DS-GVO i. V. m. § 26 Bundesdatenschutzgesetz (BDSG) gibt. Es wurde weiter erklärt, dass, sofern Einwilligungen eingeholt werden sollen, diese freiwillig sein müssen und dass er sich zu Dokumentations- und Nachweiszwecken die Aushändigung von Belehrungen oder Informationen (z. B. nach Art. 13) mit Unterschrift bestätigen lassen kann, diese dann aber keine Einwilligungen darstellen."

Fall 4:
Laufende Daten während des Beschäftigungsverhältnisses

Praktischer Fall: Frau Maier ist in der Lohnbuchhaltung der Huber AG tätig. Die Buchhaltungssoftware zeichnet bei jeder Veränderung, die Frau Maier an den Datensätzen vornimmt, mit einem Zeitstempel auf, dass Frau Maier Änderungen vorgenommen hat. Dies wird bei Aufruf des Datensatzes, gleich durch wen, mit dem Zusatz „zuletzt bearbeitet von Maier am [Datum], [Uhrzeit]" angezeigt. Frau Maier macht nach drei Jahren Betriebszugehörigkeit einen Auskunftsanspruch (nach DSGVO) gegen die Huber AG geltend, welche personenbezogenen Daten von ihr gespeichert werden.

Hier geht es um den Umfang des Auskunftsanspruches des Betroffenen (zur Löschung s. u. Fall 33), der über die Jahre eine Vielzahl von „Datenspuren" hinterlässt. Der Hessische Beauftragte für Datenschutz charakterisiert diese Datenspuren in seinem Tätigkeitsbericht 2018 wie folgt:

„Darüber hinaus emittieren Beschäftigte unter Berücksichtigung ihrer Tätigkeitsausübung Daten zu ihrer Person etwa bei der Nutzung der zur Verfügung gestellten IT-Infrastruktur (PC, Laptop, Mobiltelefon, Tablet) oder der geschäftlichen Kommunikation (Erstellung von Schriftstücken oder Kommunikation mittels E-Mail). Da das Arbeitsverhältnis naturgemäß auf eine gewisse Dauer angelegt ist, fallen diese Daten unter Umständen über Jahre und Jahrzehnte hinweg an."

Diese „Bewegungsdaten" – in Abgrenzung zu den Stammdaten – umfassen auch Protokoll- und Logging-Daten, die insbesondere bei der Benutzung von Fachapplikationen der Unternehmens-IT aufgezeichnet werden. In der SAP-Welt werden die in der Fallgestaltung oben betroffenen Daten beispielsweise als „Änderungsbelege" bezeichnet. Spezifische Fragestellungen im Zusammenhang mit der Protokollierung als solcher werden unten in Fall 38 behandelt.

- Legitimationsgrund?

Soweit diese „Bewegungsdaten" Beschäftigter im Rahmen juristischer Stellungnahmen thematisiert werden, geht es meist um Fragen im Zusammenhang mit dem Auskunftsrecht des Betroffenen. Dabei wird allerdings häufig eine grundlegendere Frage übersehen, nämlich, welche datenschutzrechtliche Legitimationsgrundlage der Erhebung dieser Daten durch den

Arbeitgeber überhaupt zugrunde liegt. Ähnlich wie bei den unternehmensbezogenen Kontaktdaten (dazu oben Fall 1) und den „Personalaktendaten“ (unten Fall 7) könnten die Daten für die Durchführung des Beschäftigungsverhältnisses erforderlich sein (§ 26 BDSG). Im Gegensatz zur alternativ anzunehmenden Interessenabwägung wäre dann z. B. ein Widerspruch des Beschäftigten gegen die Verarbeitung nicht möglich. In den einschlägigen Abhandlungen steht die Legitimität der Verarbeitung von Bewegungsdaten an sich meist außer Frage, solange es nur um die Nachvollziehbarkeit bzw. Aufklärbarkeit unternehmensinterner Vorgänge anhand dieser Daten geht und nicht um eine Überwachung des Mitarbeiters. Allerdings ist diese Grenze – die Erhebung von Bewegungsdaten wird irgendwann nicht mehr für die Durchführung des Beschäftigungsverhältnisses „erforderlich“ sein – mitunter schwer zu ziehen.

Ein Beispiel für die schwierige Grenzziehung sind die „Online/Offline“-Anzeigen bezüglich einzelner Mitarbeiter. Diese gibt es etwa in modernen (Inhouse-) IP-Telefoniesystemen mit computergestützter Anwahl einzelner Mitarbeiter, deren Status („anwesend“/„kurz abwesend seit [Uhrzeit]“/„Urlaub bis [Tag]“/„nicht anwesend“ etc.) in einem Bildschirm-Panel „live“ verfolgt werden kann. Aber auch Messenger-Software wie Whatsapp verfügt über eine „Online“- bzw. „zuletzt Online um [Uhrzeit]“-Information. Diese Bewegungsdaten sind zwar hilfreich, aber über sie kann auch eine Kontrolle über den einzelnen Mitarbeiter ausgeübt werden (zumal bei Protokollierung bzw. Speicherung), sodass aus kollektivarbeitsrechtlicher Sicht die Einführung derartiger Mechanismen eine Mitbestimmungspflicht des Betriebsrats begründen kann (§ 87 Abs. 1 Nr. 6 BetrVG).

Ein drastisches Beispiel, das im November 2019 durch die Presse geisterte, war die Anfertigung von Notizen über Beschäftigte als Resultat von „halb-privaten“ Gesprächen der Vorgesetzten mit diesen. Man könnte auch dieses Ergebnis des „verdeckten Aushorchens“ von Mitarbeitern als „Bewegungsdaten“ klassifizieren. Die Notizen wurden einheitlich in einem Ordner zusammengefasst, auf den sämtliche Vorgesetzten Zugriff hatten, was nicht dem „need to know“-Grundsatz entspricht: Allenfalls der unmittelbar Vorgesetzte ist „Befugter“ für eine Einsichtnahme (möglicherweise neben der Personalabteilung, der IT-Abteilung im Falle von Softwaremigrationen, s. dazu unten Fall 41, und in Sonder-/Ausnahmefällen weitere Personen). Das betroffene Unternehmen behauptete dann, die Notizen zur besseren Planung der Arbeitsschichten benötigt zu haben, vernichtete aber sogleich den betroffenen Ordner. Schon dies spricht natürlich dagegen, dass die Daten „für die Durchführung des Beschäftigungsverhältnisses erforderlich“ waren. Natürlich waren den betroffenen Beschäftigten auch keine Pflichthinweise über die Erhebung dieser Daten erteilt worden.

➢ Bewegungsdaten von Beschäftigten als Gegenstand eines Auskunftsanspruchs

In Vorlagen, etwa im Rahmen von Muster-Verarbeitungsverzeichnissen oder Pflichthinweisen für Beschäftigte, werden Bewegungsdaten von Beschäftigten als laufend in Systemen hinterlassene (protokollierte) Spuren häufig nicht berücksichtigt. Gleichwohl ist es vom Wortlaut der DSGVO her gesehen evident, dass es sich um personenbezogene Daten des Beschäftigten handelt, die der Arbeitgeber verarbeitet. Daher ist der Arbeitgeber im Kontext des Auskunftsrechts des Betroffenen auch bezüglich dieser Informationen im Grundsatz verpflichtet, dem Betroffenen *„eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung“* zu stellen (Art. 15 Abs. 3 DSGVO). Wie dies in der Praxis geschehen soll und ob es juristisch überzeugende Argumente gegen diese „uferlose“ Pflicht gibt, ist allerdings bislang offen.

Das Landesarbeitsgericht Baden-Württemberg hat in einem Urteil vom Dezember 2018 zu den „dienstlichen“ E-Mails – als Kommunikations- bzw. Bewegungsdaten des Beschäftigten – ausgeführt:

„Dass die Beklagte personenbezogene Daten des Klägers verarbeitet, ergibt sich schon aus der Vielzahl der von den Parteien als Ausdrucke in diesem Rechtsstreit vorgelegten dienstlichen E-Mails, die der Kläger im Rahmen seines Arbeitsverhältnisses geschrieben, gesendet und empfangen hat. Jede einzelne vom Kläger geschriebene, gesendete und empfangene E-Mail enthält bereits personenbezogene Daten, nämlich Informationen, die sich auf den Kläger beziehen. Insofern ist der Einwand der Beklagten, sie würde außerhalb der Personalakte keine Negativlisten oder dergleichen über den Kläger führen, unerheblich.“

Ähnlich führt das OLG Köln in einer Entscheidung vom Juli 2019 aus:

„Soweit die Beklagte den Begriff der personenbezogenen Daten auf die bereits mitgeteilten Stammdaten begrenzt sehen möchte und meint, eine Verpflichtung zur Beauskunftung über insbesondere elektronisch gespeicherte Vermerke zu mit dem Kläger geführten Telefonaten und sonstigen Gespräche bestehe nicht, ist ein entsprechendes Verständnis mit dem der DS-GVO zu Grunde liegenden weit gefassten Datenbegriff nicht in Einklang zu bringen. Denn durch die Entwicklung der Informationstechnologie mit ihren umfassenden Verarbeitungs- und Verknüpfungsmöglichkeiten gibt es keine belanglosen Daten mehr [...]. Soweit in Gesprächsvermerken oder Telefonnotizen Aussagen des Klägers oder Aussagen über den Kläger festgehalten sind, handelt es sich hierbei ohne weiteres um personenbezogene Daten.“

➢ Kopie der Daten, Kopie der Akte?

Von vielen Juristen werden nun mit großem Begründungsaufwand verschiedene Einschränkungen dieses „uferlosen Kopie-Herausgabeanspruchs“ diskutiert. Die Aufregung zeigt, dass es sich hier um ein praxisrelevantes Thema handelt: In Zukunft ist damit zu rechnen, dass mit Auskunftsansprüchen allerlei „befugter Unfug“ getrieben wird, um letztlich ganz andere Ziele zu erreichen als die vordergründige Auskunft. Man muss kein Prophet sein, um zu dem Schluss zu gelangen, dass Arbeitsrechtler das „uferlose“ Auskunftsrecht in Streitigkeiten zwischen Arbeitgeber und Arbeitnehmer – insbesondere natürlich bei einer (bevorstehenden) Trennung (Kündigungsschutzverfahren) – einsetzen werden, um den Arbeitgeber, vorsichtig ausgedrückt, etwas „auf Trab zu bringen“ und diesem die Schlagkräftigkeit dieses unerhofften Arbeitnehmerrechts vor Augen zu führen. Die zusätzliche Belastung beim Arbeitgeber durch diese Instrumentalisierung kann durchaus Einfluss auf dessen Vergleichsbereitschaft haben. Zu denken ist insbesondere an die Forderung der Herausgabe sämtlicher vorhandener Abrechnungen, E-Mail-Konversationen, Messenger-Chats, Login- und Protokoll-Daten. Dabei geht es natürlich in erster Linie darum, Material für die weitere Auseinandersetzung zu sammeln, zumal eine Kopie einer Vorgangsunterlage – eingeschlossen Screenshots und Originaldateien – häufig neben dem Inhalt notgedrungen auch einen Einblick in den „Verarbeitungskontext“ (verwendete Applikation etc.) liefert.

Als Arbeitgeber müsste man im Grunde darüber nachdenken, für solche Fallgestaltungen das Schikaneverbot des § 226 BGB heranziehen: *„Die Ausübung eines Rechts ist unzulässig, wenn sie nur den Zweck haben kann, einem anderen Schaden zuzufügen“*. Aber weder wird dieser Zweck beweisbar sein noch interessiert sich die DSGVO für das deutsche BGB.

Das Spektrum der diskutierten Einschränkungen beginnt bereits mit dem Argument, das Recht auf „Kopie der Daten“ meine im Grunde nur die „Auskunft über die Daten“. Das bayerische Landesamt für Datenschutzaufsicht beruft sich in seinem Tätigkeitsbericht 2017/2018 diesbezüglich auf ein Urteil des Europäischen Gerichtshofes vom Juli 2014 zur Vorgängerregelung (EU-Datenschutzrichtlinie), ohne allerdings darauf hinzuweisen, dass es das ausdrückliche Recht auf Kopie damals noch gar nicht gab. Das bayerische Landesamt führt gleichwohl kurzerhand aus:

„Nach Art. 15 Abs. 3 DS-GVO ist nur eine „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind“, zur Verfügung zu stellen. Es ist hier jedoch nicht die Rede von Kopien der betreffenden Akten, von sonstigen Unterlagen usw.“

Wie so oft geht es dabei um die von der DSGVO nicht klar beantwortete Frage, was genau eigentlich das „personenbezogene Datum“ als solches ist, über das Auskunft zu erteilen ist. Erwägungsgrund 63 drückt in diesem Zusammenhang das Verständnis der DSGVO aus, dass das Auskunftsrecht spezifische Informationen „in“ Akten betrifft, also nicht die Akten als solche. Allerdings zählt der genannte Erwägungsgrund „in“ den (Patienten-)Akten befindliche Informationen wie „Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen“ auf. Damit erscheint die Unterscheidung in eine Akte und die personenbezogenen Daten „in“ der Akte nicht nur willkürlich – weil sie an die konkrete Aufmachung und Ordnung von bzw. in Akten beim Verantwortlichen anknüpft –, sondern auch weitgehend sinnlos, wenn als Inhalt der Akte dann doch die einzelnen (im Extremfall also sämtliche) Dokumente in der Akte bezeichnet werden.

Der Europäische Gerichtshof hatte hingegen in der bereits oben erwähnten Entscheidung vom Juli 2014 zur damaligen EU-Datenschutzrichtlinie differenziert hinsichtlich der personenbezogenen Daten „in“ einem Dokument einerseits und dem Dokumenteninhalt andererseits. Konkret ging es um den (internen) Entwurf eines asylrechtlichen Bescheides, in dem die einschlägigen asylrechtlichen Vorschriften auf den konkreten Fall des Betroffenen angewandt wurden und den der Betroffene im Wege eines Auskunftsrechts einsehen sollte. Der Europäische Gerichtshof entschied seinerzeit, dass die Analyse als solche kein personenbezogenes Datum des bzw. über den Betroffenen sei, *„sondern höchstens, soweit sie sich nicht auf eine rein abstrakte Rechtsauslegung beschränkt, um eine Information darüber, wie die zuständige Behörde dieses Recht im Fall dieses Antragstellers beurteilt und anwendet, denn dieser Fall wird u. a. anhand der personenbezogenen Daten behandelt, die dieser Behörde über seine Person vorliegen“*. Der Europäische Gerichtshof fasste zusammen, dass *„es sich bei den in der Entwurfsschrift wiedergegebenen Daten über denjenigen, der einen Aufenthaltstitel beantragt, und den Daten, die ggf. in der in der Entwurfsschrift enthaltenen rechtlichen Analyse wiedergegeben sind, um „personenbezogene Daten” i. S. d. Bestimmung handelt. Diese Einstufung gilt allerdings nicht für die Analyse als solche.“*

Diese Argumentation kann durchaus die oben dargestellten Sätze des Landesarbeitsgerichts in Stuttgart sowie des OLG Köln relativieren: Die personenbezogenen Daten sind damit nicht die Korrespondenz oder der Vermerk als solcher, sondern nur die darin (als „Tatsachengrundlage“ bzw. „Identifikationsinformation“) enthaltenen Daten über die Person. Nach diesem Urteil des Europäischen Gerichtshofes ist die in einer E-Mail enthaltene Information „Tante Ida hat heute Geburtstag“ kein personenbezogenes Datum des E-Mail-Absenders – auch wenn er dies an einem bestimmten Tag um eine bestimmte Uhrzeit geschrieben hat – , sondern einzig ein solches von „Tante Ida“ selbst. Daher würde dieses personenbezogene

Datum, selbst wenn es der E-Mail-Absender „verfasst“ hat, nicht Gegenstand des datenschutzrechtlichen Auskunftsanspruchs sein. Sicherlich ist aber der Umstand als solcher, dass der E-Mail-Absender an einem bestimmten Tag um eine bestimmte Uhrzeit von einem bestimmten Account aus eine E-Mail geschrieben hat, ein personenbezogenes Datum, da es etwas darüber aussagt, was diese Person zu diesem Zeitpunkt gemacht hat.

Das Landgericht Köln hat in einer Entscheidung vom März 2019 zwischen den Personendaten, den Identifizierungsmerkmalen, dem Akteninhalt, internen Vorgängen und „Doppelübersendungen“ differenziert und bestätigt im Kontext der DSGVO das Urteil des Europäischen Gerichtshofs vom Juli 2014 im Hinblick auf (interne) rechtliche Bewertungen und Analysen:

„Insofern ergibt sich ein umfassendes Auskunftsrecht bezogen auf die gespeicherten bzw. verarbeiteten personenbezogenen Daten. Dies beinhaltet Daten wie Namen oder Geburtsdatum genauso wie jegliche Merkmale, die die Identifizierbarkeit einer Person ermöglichen können, z. B. Gesundheitsdaten, Kontonummer usw. Nach diesen Grundsätzen und auf Grundlage der Erwägungsgründe stellen ärztliche Unterlagen, Gutachten oder sonstige vergleichbare Mitteilungen anderer Quellen ebenfalls „personenbezogene Daten“ dar. Nach der Auffassung der Kammer bezieht sich der Auskunftsanspruch aber nicht auf sämtliche internen Vorgänge der Beklagten, wie z. B. Vermerke, oder darauf, dass die betreffende Person sämtlichen gewechselten Schriftverkehr, der dem Betroffenen bereits bekannt ist, erneut ausgedruckt und übersendet erhalten kann [...]. Rechtliche Bewertungen oder Analysen stellen insofern ebenfalls keine personenbezogenen Daten in diesem Sinne dar. Der Anspruch aus Art. 15 DS-GVO dient nicht der vereinfachten Buchführung des Betroffenen, sondern soll sicherstellen, dass der Betroffene den Umfang und Inhalt der gespeicherten personenbezogenen Daten beurteilen kann.“

Soweit hier mit dem Betroffenen bereits gewechselter Schriftverkehr von einer (erneuten) Kopie ausgenommen wird, könnte man auch sagen: Der Verantwortliche ist nicht das (Zwangs-)Archiv des Betroffenen. Das klingt zwar einleuchtend, steht aber im Widerspruch zu anderen Regelungen der DSGVO, wonach der Betroffene selbst dann, wenn die Daten eigentlich gelöscht werden müssten, „die Löschung der personenbezogenen Daten ablehnen“ kann (Art. 18 Abs. 1 lit. b DSGVO), etwa weil er sie „zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt“ (Art. 18 Abs. 1 lit. c DSGVO). Der DSGVO ist also der Speicher- und Rechercheaufwand beim Verantwortlichen gelinde gesagt nicht so wichtig (s. dazu auch unten Fall 28).

Im Gegensatz zu den „internen“ Vermerken und Analysen sind „externe“ Dokumente aber aus Sicht des Landgerichts Köln „herausgabepflichtig“. Ähnlich hat auch das Kammergericht in Berlin in einer Entscheidung vom Oktober 2018 die Herausgabe eines (kompletten) medizinisches Gutachtens, das eine Versicherung über den Betroffenen (ihren Versicherungsnehmer) eingeholt hatte, auf den datenschutzrechtlichen Auskunftsanspruch gestützt. Dabei hat das Kammergericht zugleich darauf hingewiesen, dass dieser konkrete Anspruch (und zwar aus vertraglichen Nebenpflichten) auch vor der Einführung der DSGVO bereits bestanden hatte.

Der Hessische Beauftragte für Datenschutz sieht dies in seinem Tätigkeitsbericht 2018 differenzierter:

„Einen Anspruch auf Herausgabe einzelner Kopien – z. B. im Sinne einer Fotokopie bestimmter Dokumente – enthält Art. 15 Abs. 3 DS-GVO in aller Regel nicht: Die Pflicht, eine Kopie zur Verfügung zu stellen, ist nicht mit einem allgemeinem Recht auf Zugang zu Informationen oder einem Akteneinsichtsrecht gleichzusetzen. Gleichwohl können Verantwortliche im Einzelfall auch zur Übersendung einer Fotokopie eines bestimmten Dokuments verpflichtet sein. Dies kann dann der Fall sein, wenn das Recht der Betroffenen, die Rechtmäßigkeit der Datenverarbeitung eigenständig zu überprüfen, untrennbar hiermit verbunden ist.“

Eine solches, abstrakt beschriebenes Regel-Ausnahme-Verhältnis, das so nicht aus dem Wortlaut der DSGVO ableitbar ist, stellt zwar konsequent auf den Blickwinkel des Betroffenen und seines „Rechts auf Prüfung der Rechtmäßigkeit der Datenverarbeitung“ ab, gibt dem Verantwortlichen aber keine Richtschnur an die Hand. Wenn ein interner Untersuchungsbericht über einen Mitarbeiter (natürlich) den Namen des Mitarbeiters enthält, wann kann dann der Mitarbeiter die Rechtmäßigkeit dieser Datenverarbeitung nur überprüfen, wenn er den Untersuchungsbericht als Ganzes erhält? In Wirklichkeit wird das dem Betroffenen auch herzlich egal sein: Er wird einfach lesen wollen, was in dem Bericht über ihn steht.

Kann der Betroffene hiernach eine Kopie verlangen, so ist ihm diese nach Meinung des Hessischen Beauftragten für Datenschutz ohne gesonderte Aufforderung zur Verfügung zu stellen, d. h. der Verantwortliche muss diese Frage „für sich selbst“ durchaus bei jedem geltend gemachten Auskunftsanspruch lösen:

„Verantwortliche müssen der in Art. 15 Abs. 3 DS-GVO enthaltenen Verpflichtung daher auch ohne entsprechenden Hinweis der Betroffenen nachkommen.“

Der Verantwortliche kann sich nach einem Urteil des AG München die Arbeit auch nicht durch die Bitte um Präzisierung des Auskunftsverlangen des Betroffenen erleichtern:

„Der Ansatz der Beklagtenseite, auf die eigene Auskunftsbereitschaft zu verweisen, jedoch den Kläger aufzufordern, näher auszuführen, welche konkreten Daten begehrt werden, da eine unterschiedslose und flächendeckende Auswertung des gesamten auf Seiten der Beklagten vorhandenen Datenbestands einen erheblichen Aufwand von mehreren Manntagen auslösen würde, geht am Schutzzweck der Norm vorbei und zwar auch in den Fällen, wie dem vorliegenden, in denen die Klagepartei zulässigerweise ein vollständiges Auskunftsersuchen stellt.“

Da die Verletzung des Auskunftsrechts des Betroffenen (natürlich) bußgeldbewehrt ist, wird der Verantwortliche, wenn er auf der sicheren Seite sein und sich nicht auf Diskussionen über die vom Hessischen Beauftragten für Datenschutz ins Feld geführte „Untrennbarkeit der Übersendung einer Kopie eines Dokuments mit dem Recht des Betroffenen zur eigenständigen Überprüfung der Rechtmäßigkeit der Datenverarbeitung“ einlassen will, alle Dokumente zur Verfügung stellen. Das wird in der Praxis das vom Hessischen Beauftragten für Datenschutz anvisierte Regel-Ausnahme-Verhältnis in sein Gegenteil verkehren.

Man erkennt an dieser Stelle: Der DSGVO-Gesetzgeber ging offensichtlich von der (naiven) Vorstellung aus, dass „die personenbezogenen Daten eines Betroffenen“ in einer (einzelnen) Datei aufbewahrt werden, auf die der Verantwortliche eine Art „Fernzugriff“ einräumen kann. Mit einer solchen Konzeption im Hinterkopf lässt sich natürlich einfach eine Auskunft erteilen (Ausdruck der Datei), eine Kopie zur Verfügung stellen (Übersendung der Datei im „Quellformat“) und durch Konvertierung in ein allgemein gebräuchliches Format lässt sich das Recht auf Datenübertragbarkeit erfüllen. Ein Autor des Gesetzes würde nun natürlich trotzig sagen, dass sich die beim Verantwortlichen vorhandene, komplexe IT-Landschaft dann eben diesem Konzept zu beugen haben – „was nicht passt, wird passend gemacht“.

Besonders kommt dieser letztgenannte Gedanke in einem Ausspruch des OLG Köln in einem Urteil aus dem Juli 2019 zum Ausdruck:

„Soweit die Beklagte meint, es sei für Großunternehmen, die wie sie einen umfangreichen Datenbestand verwalten würden, mit den ihr zur Verfügung stehenden Ressourcen wirtschaftlich unmöglich, Dateien auf personenbezogene Daten zu durchsuchen und zu si-

chern, verfängt dies nicht. Es ist Sache der Beklagten, die sich der elektronischen Datenverarbeitung bedient, diese im Einklang mit der Rechtsordnung zu organisieren und insbesondere dafür Sorge zu tragen, dass dem Datenschutz und den sich hieraus ergebenden Rechten Dritter Rechnung getragen wird.“

- Zusammenfassung der Daten/Unterlagen?

Aber der Hessische Beauftragte für Datenschutz geht in seinem Tätigkeitsbericht 2018 noch darüber hinaus, indem er – über die ggf. zu übersendenden Kopien hinaus – die Verpflichtung des Verantwortlichen zum Zusammenfassen der „Akteninformationen“ fordert:

„Die Auskünfte müssen präzise, transparent, verständlich und leicht zugänglich in einer klaren und einfachen Sprache formuliert sein. Das „Abspeisen“ durch kommentarlose Überlassung von Kopien ist grundsätzlich nicht zulässig. Daraus folgt, dass Art. 15 Abs. 3 DS-GVO kein zusätzliches Recht auf Überlassung einer Kopie der personenbezogenen Daten meint, sondern voraussetzt, dass dem Auskunftsanspruch nach Art. 15 Abs. 1 DSGVO die Überlassung einer Kopie ausreicht. [...] Ich verstehe den Kopie-Begriff des Art. 15 Abs. 3 DS-GVO im Sinne einer sinnvoll strukturierten Zusammenfassung. Den Betroffenen müssen daher nicht sämtliche, sie betreffende Dokumente in Kopie zur Verfügung gestellt werden.“

Der oben exemplarisch genannte interne Untersuchungsbericht über den Betroffenen müsste dann also – wenn die oben postulierten Voraussetzungen für die Übersendung einer Kopie nicht vorliegen oder auch dann? – in einer klaren und einfachen Sprache für den Betroffenen zusammengefasst werden. Der Hessische Beauftragte für Datenschutz bezieht diese Pflicht zur Anfertigung einer „strukturierten Zusammenfassung“ in seinem Tätigkeitsbericht 2018 auch ausdrücklich auf Beschäftigtendaten in Form von Bewegungsdaten. Zum Inhalt der Zusammenfassung führt er konkretisierend aus:

„Welche Vorgehensweise hierbei besonders geeignet erscheint, hängt von der zu beurteilenden Datenverarbeitung, mithin von den Umständen des Einzelfalls ab. In den folgenden Konstellationen habe ich angenommen, dass den Anforderungen des Art. 15 Abs. 3 DS-GVO genüge getan ist:

- *Bereitstellung eines Auszugs des Profils von Betroffenen bei Nutzung eines Personalinformationssystems durch Verantwortliche*

- *Liste der zu einer Person gespeicherten Schriftstücke oder Aktenzeichen bei Nutzung eines Dokumentenmanagement- oder Registratursystems*

Sofern mit Verweis auf Art. 15 Abs. 3 DS-GVO die Kopie einzelner Schriftstücke oder E-Mail-Korrespondenzen verlangt wird, kann dieser Anspruch dann bestehen, wenn das Recht der Betroffenen, die Rechtmäßigkeit der Datenverarbeitung eigenständig zu überprüfen, untrennbar hiermit verbunden ist. Bei einer Zusammenschau von Art. 15 Abs. 1 und 3 DS-GVO und vor dem Hintergrund der Bedeutung des Auskunftsrechts dürfte es nach meinem Verständnis in aller Regel genügen, wenn den Betroffenen die in einem Schriftstück enthaltenen personenbezogenen Daten mitgeteilt werden. Die Kopie eines Schriftstücks/einer E-Mail muss jedoch in der Regel nicht zur Verfügung gestellt werden."

Glücklich, wer daraus eine klare Vorgabe für die den Auskunftsanspruch bearbeitenden Mitarbeiter oder Systeme in einem Unternehmen ableiten kann, insbesondere wenn ein „Massenverkehr" mit Auskunftsansprüchen droht.

- Archivdaten

Andere Argumentationen, die ein eigenständiges Recht auf „Kopie der Daten" anerkennen, beschäftigen sich etwa mit Einschränkungen bezüglich der Herausgabe von Back-up-Daten bzw. von „Aufbewahrungsdaten" (d. h. von Daten, die nur noch zu Aufbewahrungszwecken gespeichert werden). § 34 BDSG gibt in diesem Zusammenhang explizit vor, dass kein Auskunftsrecht besteht, wenn die Daten

„nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist."

Natürlich wird – wie bei jeder nationalen Norm im Regelungsbereich der DSGVO – die Europarechtswidrigkeit dieser Vorschrift ins Feld geführt. Wenn ein Verantwortlicher die Daten „hat", muss er Auskunft darüber erteilen, auch wenn sie im Archiv im Keller liegen, lautet das Argument.

- Daten Dritter

Nach Art. 15 Abs. 4 DSGVO müssen bei der Herausgabe von Kopien „die Rechte und Freiheiten anderer Personen" beachtet werden. Die Herausgabe kann also insoweit verweigert

werden, als dadurch Drittrechte bzw. Drittdaten an den Betroffenen als „Unbefugten“ herausgegeben werden würden. Der Teufel steckt hier im Wörtchen „insoweit“.

Im Fall des Landesarbeitsgerichts Stuttgart (s. o.) weigerte sich die Beklagte (d. h. der Verantwortliche) etwa, eine Kopie sämtlicher Informationen über den Betroffenen (einschließlich intern verfasster Berichte, die den Betroffenen „betreffen“) herauszugeben mit dem Argument, dass der Herausgabeanspruch durch die Rechte und Freiheiten anderer Personen beschränkt sei. Das Landesarbeitsgericht führte aus, dieser Hinweis sei in seiner Pauschalität keine taugliche Verteidigung:

„Es bedürfte der Nennung eines konkreten Sachverhaltes, anhand dessen geprüft werden könnte, ob durch die Auskunftserteilung tatsächlich die Rechte und Freiheiten anderer Personen beschränkt werden würde. Die Einschränkung des Auskunftsanspruches wegen überwiegender schützenswerter Interessen Dritter scheitert bereits daran, dass es nach dem Vortrag der Beklagten unklar bleibt, auf welche personenbezogenen Daten des Klägers sich die behaupteten schützenswerten Interessen Dritter beziehen sollen. Soweit die Beklagte mit dem Hinweis auf schützenswerte Interessen Dritter den Auskunftsanspruch verweigert, ist sie für die maßgeblichen Umstände in der Darlegungslast. Sie wäre kraft Sachnähe in der Lage gewesen, vorzutragen, welche konkreten personenbezogen Daten nicht herausgegeben werden können, ohne dass schützenswerte Interessen Dritter tangiert werden. Zu dieser Darlegung hätten nicht schon die personenbezogenen Daten als solche preisgegeben werden müssen. Ausreichend, aber auch erforderlich wäre gewesen, darzulegen, auf welche genauen Informationen (Sachverhalt/Vorfall/Thema in zeitlicher und örtlicher Eingrenzung nebst handelnden Personen) sich das überwiegende berechtigte Interesse an einer Geheimhaltung beziehen soll. Nur dann wäre der Kammer die notwendige Einzelfallabwägung möglich gewesen. Soweit in diesem Fall die berechtigten Interessen Dritter gegenüber dem Auskunftsinteresse des Klägers überwogen hätte, wäre auch erst dann in einem zweiten Schritt eine gegenständliche Einschränkung im Tenor möglich gewesen.“

Muss also die den Betroffenen betreffende Information herausgegeben werden, so hat die oben dargestellte Auffassung des Hessischen Beauftragten für Datenschutz, dass Unterlagen im Rahmen des Auskunftsanspruchs für den Betroffenen zusammenzufassen sind, durchaus Vorzüge. Beispielhaft kann man sich hier einen „Mittäter“ einer Pflichtverletzung im Unternehmen vorstellen, der in einem internen Untersuchungsbericht genannt wird, als solchen Dritten vorstellen, aber auch den Urheber (Autor) des Untersuchungsberichts selbst. Nach landläufigem Verständnis müssten nun die Angaben über solche Dritte sorgfältig geschwärzt

werden. Der Hessische Beauftragte für Datenschutz führt dazu in seinem Tätigkeitsbericht 2018 aus:

„Werden den Betroffenen Kopien von Schriftstücken oder Dokumenten zur Verfügung gestellt, so kann sich bei mangelnder Sorgfalt das Risiko erhöhen, dass den Betroffenen auch Informationen zur Verfügung gestellt werden, die möglicherweise Rechte Dritter tangieren. Fertigen Verantwortliche hingegen eine strukturierte Zusammenfassung und tragen hierbei die personenbezogenen Daten der Betroffenen eigenständig zusammen, ist dieses Risiko deutlich minimiert."

Das hier postulierte „Recht auf Zusammenfassung" wird allerdings an anderer Stelle im selben Tätigkeitsbericht wieder eingeschränkt:

„Sofern personenbezogene Daten der Betroffenen in Datenverarbeitungen gespeichert sind, die nicht der Verarbeitung von Beschäftigtendaten dienen, sondern anderen Zwecken (z. B. Verarbeitung von Kundendaten) und somit nicht in Bezug auf den Anspruchssteller verarbeitet werden, genügt es, wenn Verantwortliche die Informationen nach Art. 15 Abs. 1 lit. a bis h DS-GVO zur Verfügung stellen und den Betroffenen die Möglichkeit einräumen, eine Präzisierung ihres Auskunftsersuchens vorzunehmen."

Nach dieser Auffassung ist also inhaltlich zwischen „mitarbeiterbezogenen" und „kundenbezogenen" (bzw. „lieferantenbezogenen") Daten des Beschäftigten zu unterscheiden. In letzterem Fall gibt es – zumindest zunächst – kein Recht auf eine Kopie oder Zusammenfassung. Aus der DSGVO lässt sich dies so nicht herleiten: Zwar darf *„das Recht auf Erhalt einer Kopie die Rechte und Freiheiten anderer Personen nicht beeinträchtigen"* aber das bedeutet nicht, dass ein E-Mail-Verkehr zwischen einem Mitarbeiter und einem Kunden (bzw. dem Mitarbeiter eines Kunden) – der unzweifelhaft ein personenbezogenes Datum des Mitarbeiters ist – nicht auch geschwärzt herausgegeben oder zusammengefasst werden könnte. Vermutlich hat hier der Hessische Beauftragte für Datenschutz den Argwohn gehabt, dass es unverhältnismäßig wäre, wenn jede Korrespondenz zwischen dem Beschäftigten und „irgendjemandem" auch noch (in einer Zusammenfassung) vorgelegt werden müsste. Deshalb wurde hier die uferlose Formulierung des Auskunftsanspruchs – wie eine aus der Form geratene Hecke – etwas „zurechtgestutzt". Ähnlich haben auch andere Datenschutzbehörden (bzw. einzelne ihrer Vertreter) in diesem Zusammenhang erklärt, das Auskunftsrecht der Betroffenen beziehe sich nur auf die „Stammdaten". Diese Einschränkungen sind dem Text der DSGVO allerdings nicht zu entnehmen. Solche Vorschläge korrigieren eine „uferlose" Regelung, in der an Bewegungsdaten von Beschäftigten, die sich im Laufe der Zeit auftürmen,

überhaupt nicht gedacht wurde, und die nun zu „uferlosen“ Ergebnissen führt und dementsprechend missbraucht werden kann.

Auch die Herausgabe von Betriebs- und Geschäftsgeheimnissen des Verantwortlichen kann möglicherweise die „Rechte und Freiheiten anderer Personen“ beeinträchtigen, hier diejenigen des Verantwortlichen selbst. Alternativ kann der Verantwortliche auch Geheimhaltungspflichten gegenüber Dritten unterliegen, die er einhalten möchte (Pflichtenkollision). Letztlich ist aber offen, ob auch der Verantwortliche selbst oder dessen Geschäftspartner (also insbesondere eine Gesellschaft bzw. juristische Person) eine „andere Person“ im Sinne des Art. 15 Abs. 4 DSGVO sein kann und damit die Pflicht zur Herausgabe von Kopien (wegen dessen Rechten) beschränkt werden muss bzw. darf. Das OLG Köln hat in seiner Entscheidung vom Juli 2019 zumindest für Daten, die vom Betroffenen selbst stammen, klargestellt, dass deren Herausgabe nicht mit der Begründung eines entsprechenden Geschäftsgeheimnisses des Verantwortlichen verweigert werden kann:

„Die Beklagte kann sich demgegenüber auch nicht mit Erfolg darauf berufen, dass ein entsprechend weit gefasster Datenbegriff ihre Geschäftsgeheimnisse verletzen würde. Ungeachtet aller sonstigen sich stellenden Fragen gilt dies schon deshalb, weil Angaben, die der Kläger selbst gegenüber seiner Versicherung gemacht hat, diesem gegenüber nicht schutzbedürftig und damit auch nicht ihr Geschäftsgeheimnis sein können.“

- Wie präzise müssen die Daten gefordert werden?

Neben diesen unzusammenhängenden Äußerungen von Gerichten und Behörden werden in der juristischen Literatur weitere Einschränkungen des Rechts auf Auskunft etwa bei „unpräzisen Herausgabeersuchen“ befürwortet. Dieser Einwand soll Auskunfts- und Kopie-Ersuchen wie „bitte alle Daten über mich vorlegen“ entgegengestellt werden können. Nur wie soll der Betroffene wissen, wonach er fragen soll, wenn er nicht weiß, was alles verarbeitet wird? Auch unverhältnismäßiger Aufwand bei der Identifikation der maßgeblichen Daten soll eine Grenze des Herausgabeanspruches darstellen. Je konkreter die Anfrage ist (bzw. fokussiert gestellt wurde), desto mehr Aufwand soll zumutbar sein. Eventuell soll auch die Intensität der personenbezogenen Daten in einem Dokument maßgeblich sein: Wird der Betroffene nur „erwähnt“, soll kein Herausgabeanspruch bestehen; anders, wenn „signifikante biografische Informationen“ im Dokument vorhanden sind. So sollen Personal-, Kranken- oder Kundenakten „hinreichend personenbezogen“ sein, geschäftliche Sitzungs- oder Besprechungsprotokolle jedoch nicht. E-Mail-Korrespondenz mit Leistungsbeurteilungen über den Betroffenen soll erfasst sein, Protokolle über Kundengespräche, die vom Betroffenen verfasst wurden, jedoch nicht.

Wieder einmal muss die mangelnde Präzision und Vorausschau bzw. Umsichtigkeit der DSGVO, die eben überwiegend aus abstrakten und scheinbar grenzenlosen Prinzipien besteht, durch eine mühsame, kleinteilige Definitionsarbeit ohne jegliche Rechtssicherheit ergänzt werden. Jedes Urteil zu diesen Fragen wird – wie auch insbesondere die oben erwähnte Entscheidung des Landesarbeitsgerichts Baden-Württemberg – neue Fragen aufwerfen. Der Traum jedes Juristen – und der Alptraum jedes Rechtsanwenders, der sich eigentlich mit anderen Dingen beschäftigen möchte.

- Recht auf Datenübertragbarkeit

Es könnte überdies auch sein, dass die im Ausgangsfall genannten Bewegungsdaten von Frau Maier „auf einem Vertrag", nämlich dem Beschäftigungsverhältnis, „beruhen", und dem Verantwortlichen (Arbeitgeber) „bereitgestellt" wurden, sodass diese Daten zusätzlich dem Recht auf Datenübertragbarkeit (Art. 20 DSGVO) unterliegen. Sie wären dann nicht nur – wie im Falle des Auskunftsrechts – unstrukturiert (und möglicherweise als Ausdruck) zur Verfügung zu stellen, sondern „in einem strukturierten, gängigen und maschinenlesbaren Format". Die Datenschutzbehörden gehen generell davon aus, dass auch „nachverfolgte" Daten von der betroffenen Person bei der Nutzung des Geräts „bereitgestellt" werden. Der Verantwortliche müsste also solche Protokolldaten, die teils „nur" Bestandteil einer größeren Datenbank sind, sowie sämtliche Kommunikationsdaten gezielt als solche in strukturierter Form exportieren können.

Zum Schluss noch der Hinweis, dass das Vorstehende nur die datenschutzrechtliche Dimension der Herausgabe von Informationen (personenbezogenen Daten) betrifft. Ob ein Mandant Anspruch auf Herausgabe „seiner" Akte, die der Rechtsanwalt führt, der Patient Anspruch auf Herausgabe „seiner" (vollständigen) Patientenakte, der Informationssuchende im Rahmen der Informationsfreiheitsgesetze Anspruch auf Herausgabe von Akten der öffentlichen Verwaltung hat, ist eine ganz andere, hier nicht besprochene Dimension, die zu anderen (weitergehenden) Ergebnissen führen kann.

Fall 5:
Muss einem Dritten bei Weitergabe seiner Daten innerhalb des Konzerns diese Übermittlung mitgeteilt werden?

Praktischer Fall: Die Maier GmbH ist eine Tochtergesellschaft der Huber AG. Herr Schulze, ein freiberuflicher Programmierer, der für die Maier GmbH Software programmiert hat, fordert seine Vergütung von der Maier GmbH inkl. Verzugszinsen ein, während die Maier GmbH Mängel der programmierten Software geltend macht und die Zahlung verweigert bzw. mit Schadensersatzansprüchen aufrechnet. Das Rechnungswesen der Huber AG erstellt traditionell auch den Jahresabschluss der Maier GmbH und fragt nun für das hier maßgebliche Jahr detaillierte Informationen über das Verhältnis zwischen der Maier GmbH und Herrn Schulze ab, um die Notwendigkeit der Einstellung entsprechender Verbindlichkeiten/Rückstellungen in den Jahresabschluss der Maier GmbH bewerten zu können. Die Maier GmbH stellt der Huber AG die maßgeblichen Informationen, darunter auch Namen und Korrespondenz mit Herrn Schulze, zur Verfügung.

Zum Hintergrundverständnis dieses Falles ist zunächst folgender Gedankengang hilfreich: Der Gesetzgeber geht davon aus, dass die Übermittlung von personenbezogenen Daten Dritter (etwa einer aktuellen oder künftigen „Gegenpartei") durch einen Mandanten an einen Berufsgeheimnisträger – Rechtsanwalt, Wirtschaftsprüfer, Steuerberater – eine Zweckänderung darstellt. Das klingt nachvollziehbar, denn in den wenigsten Fällen werden Daten von vornherein vom ursprünglichen Verantwortlichen bei einem Dritten (z. B. einem Vertragspartner) beispielsweise zu dem Zweck erhoben, die rechtlichen Möglichkeiten oder Risiken eines Vorgehens gegen den Vertragspartner (oder umgekehrt gegen den Verantwortlichen) bewerten zu lassen und zu diesem Zweck Daten an einen Rechtsanwalt weiterzugeben. Gerade diese Zweckänderung löst jedoch eigentlich Informationspflichten des übermittelnden Mandanten (zum Übermittlungsempfänger siehe oben Fall 1) gegenüber dem Betroffenen über die Zweckänderung und das weitere Schicksal der Daten aus (Art. 13 Abs. 3 DSGVO). Der deutsche Gesetzgeber „erlässt" dem Mandanten diese Informationspflicht gegenüber dem Betroffenen im Falle einer Zweckänderung gleichwohl, wenn die Daten an einen Berufsgeheimnisträger übermittelt werden (§ 29 Abs. 2 BDSG).

Der Hintergrund dieser Regelung liegt auf der Hand: Der Mandant soll sich ungestört einen Rat über sein Verhältnis zum Dritten vom Berufsgeheimnisträger einholen dürfen, ohne den Dritten vorwarnen zu müssen. Auch der Berufsgeheimnisträger, der die Daten des Dritten übermittelt erhält, „erhebt" sie eventuell gar nicht (siehe oben Fall 1) und muss daher den Dritten auch nicht (nach Art. 14 DSGVO) benachrichtigen. Selbst wenn man den Empfang

als Erhebung ansieht, kann der Berufsgeheimnisträger wohl im Regelfall nach § 29 Abs. 1 BDSG von einer Erteilung der Pflichthinweise an den Betroffenen absehen.

Nach einer ähnlichen Regelung gilt dieser „Erlass" der Verpflichtung zur Informierung des Betroffenen bei Zweckänderung auch dann, wenn die Daten nicht an einen Berufsgeheimnisträger weitergegeben, sondern allgemein zu einem anderen Zweck weiterverarbeitet (d. h. auch an einen anderen Verantwortlichen übermittelt) werden sollen, sofern eine Information darüber an den Betroffenen „die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde" (§ 32 Abs. 1 Nr. 4 BDSG). Im Unterschied zur Übermittlung an einen Berufsgeheimnisträger ist der „Erlass" der Informationsverpflichtung bei Zweckänderung demnach hier an inhaltliche Voraussetzungen gekoppelt. Es stellt sich damit die Frage, ob eine Information der Maier GmbH an Herrn Schulze, dass die das bestehende Freiberuflerverhältnis betreffenden (personenbezogenen) Daten zu Zwecken der Verbindlichkeits-/Rückstellungsprüfung an die Huber AG übermittelt werden sollen, „die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde". Damit würde gegenüber Herrn Schulze transparent, dass eine Bewertung „seiner" vertraglichen Ansprüche bzw. Verpflichtungen bei der Huber AG stattfindet. Diese Bewertung findet im Rahmen einer Jahresabschlusserstellung jedoch typischerweise statt, stellt also kein besonderes Geheimnis dar und dürfte damit auch die Ansprüche der Maier GmbH bzw. die Schlagkraft der zugrunde liegenden Argumente nicht beeinträchtigen. Eine Besorgnis beispielsweise, Herr Schulze könnte durch die Information Vermögen verschieben, wird sich aus einer solchen Mitteilung an Herrn Schulze nicht ergeben können. Eine Mitteilung über die bevorstehende Zweckänderung, die in der Übermittlung an die Huber AG liegt, muss also stattfinden. Dies wäre, wie oben dargestellt, nicht der Fall, wenn die Daten zur Jahresabschlusserstellung an einen Wirtschaftsprüfer/Steuerberater als Berufsgeheimnisträger übermittelt werden würden.

Dabei ist allerdings wichtig, dass die beiden genannten Regelungen zum „Erlass" der Informationspflicht gegenüber dem Betroffenen bei Zweckänderung nur diese eine Pflicht entfallen lassen. Weder die Frage, ob die Zweckänderung als solche erlaubt ist, noch die Frage, welche datenschutzrechtliche Legitimationsgrundlage für die Übermittlung unter dem neuen Zweck notwendig bzw. einschlägig ist, werden hierdurch beantwortet. Zunächst muss der neue Zweck zum alten Zweck „kompatibel" sein, was sich nach den kryptischen (und nicht abschließenden) Kriterien in Art. 6 Abs. 4 DSGVO richtet. Gesetzt den Fall, eine Zweckkompatibilität liegt vor, wird für die Verarbeitung unter dem neuen Zweck eine neue datenschutzrechtliche Legitimationsgrundlage benötigt. Dabei ist offen, ob der genannte Art. 6

Abs. 4 DSGVO selbst eine solche Legitimationsgrundlage darstellt oder ob eine neue Legitimationsgrundlage für die Verarbeitung zum neuen Zweck in Art. 6 Abs. 1 DSGVO gesucht werden muss. Zwar besagt Erwägungsgrund 50, dass bei zweckändernden Weiterverarbeitungen „keine andere gesonderte Rechtsgrundlage erforderlich (ist) als diejenige für die Erhebung der personenbezogenen Daten". Doch manche Juristen halten dies für ein „Redaktionsversehen", d. h. im Zuge verschiedener Entwurfsfassungen sei da etwas durcheinander geraten. Geht man davon aus, dass eine eigenständige Legitimationsgrundlage nach Art. 6 Abs. 1 DSGVO für die Verarbeitung unter dem neuen Zweck gefunden werden muss, wird diese in der überwiegenden Zahl derartiger Fälle mit einer Interessenabwägung begründet werden müssen (Art. 6 Abs. 1 S. 1 lit. f DSGVO). Ist aber die Übermittlung der Dokumente an die Huber AG gerade mit den personenbezogenen Daten von Herrn Schulze „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich"? Oder genügt es nicht vielmehr, die Dokumente zu schwärzen, da die Identität von Herrn Schulze für die Bewertung durch das Rechnungswesen der Huber AG irrelevant ist? Bei jeder Verarbeitung, also auch bei der Übermittlung, personenbezogener Daten muss ihr Umfang „auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt" sein (Art. 5 Abs. 1 lit. c DSGVO). Pseudonymisierung und Anonymisierung (insbesondere Schwärzung) sind Mittel, um die Verarbeitung personenbezogener Daten auf das notwendige Maß zu beschränken.

Die unklare Reichweite der Legitimationsgrundlage führt zu weitergehenden Fragen, nicht nur im obigen Beispielsfall, sondern generell bei der Übermittlung personenbezogener Daten an Konzernunternehmen oder Berufsgeheimnisträger. Ob die Übermittlung zum jeweiligen Zeitpunkt im Sinne der Interessenabwägung „erforderlich" bzw. im Sinne des Gebots der Datenminimierung „notwendig" ist (oder nicht auch eine anonyme oder pseudonyme Übermittlung ausreichend ist), muss jeweils im Einzelfall geprüft werden (s. dazu auch unten Fall 41). Im Rahmen der Übermittlung an eine Konzernrechtsabteilung werden – insbesondere zur Prüfung der Rechtslage – personenbezogene Daten von Beschäftigten (wie etwa Anstellungsverträge, Abmahnungen oder Personenlisten) häufig mit „Klarnamen" weitergeleitet. Dasselbe gilt für die Überlassung von Beschäftigtendaten an einen Berufsgeheimnisträger im Rahmen der Jahresabschlusserstellung oder Jahresabschlussprüfung.

Oder: Teilt ein Mandant, der eine natürliche Person ist, einem Berufsgeheimnisträger personenbezogene Daten über einen Familienangehörigen mit, so stellt sich die Frage, ob er bei dieser Datenweitergabe noch eine „ausschließlich persönliche oder private Tätigkeit" im Sinne von Art. 2 Abs. 2 lit. c DSGVO ausübt oder nicht selbst Verantwortlicher im Sinne der DSGVO ist bzw. wird. Bisweilen, etwa bei der Übermittlung besonderer Kategorien personenbezogener Daten (insbesondere Gesundheitsdaten), scheidet die Interessenabwägung

auch als Legitimationsgrundlage gänzlich aus und es ist eine gesonderte Einwilligung des Betroffenen notwendig. Dies zeigt die Schwierigkeit der Legitimationsgrundlage „Interessenabwägung“ in einer schnelllebigen, auf Standardprozesse verengten Massendatenpraxis auf: Das von der DSGVO „verordnete Grübeln über jeden Einzelfall“ stößt damit schnell an seine Grenzen.

Fall 6:
Müssen auch interne Übermittlungsempfänger im Rahmen der Pflichthinweise angegeben werden?

Praktischer Fall: Die Huber AG klärt ihre Kunden, an die sie ihre Produkte veräußert, darüber auf, dass deren Daten mit Ausnahme von Transportdienstleistern nicht an Dritte weitergegeben werden. Die Kunden der Huber AG sind teils Unternehmen, teils natürliche Personen. Intern haben sämtliche Abteilungen der Huber AG auf die Kundendaten Zugriff, etwa die Verkaufsabteilung, die Buchhaltung, das Controlling, die Marketing-Abteilung, die Personalabteilung und die Abteilung zur Verwaltung der Huber-AG-eigenen Immobilien.

Es ist ohnehin schon im Ausgangspunkt nicht ganz trivial, der DSGVO konkrete Vorgaben dafür zu entlocken, wie intern beim Verantwortlichen mit personenbezogenen Daten umzugehen ist. Landläufig wird in diesem Kontext mit dem sogenannten „need to know"-Prinzip argumentiert: Nur derjenige, bei dessen unternehmensinterner Rolle der Umgang mit den konkreten Daten erforderlich ist, soll auf diese Daten Zugriff haben. In der DSGVO ist (nur) von „unbefugter Offenlegung " bzw. „unbefugtem Zugang" die Rede und dabei ist weder definiert, ob sich dies auch auf das „Innenleben" des Verantwortlichen bezieht noch, was „befugt" im Innenleben eines Verantwortlichen genau bedeutet.

Unklar ist aber darüber hinaus auch, ob eine Abteilung im Verhältnis zu einer anderen Abteilung eine „andere Stelle" sein kann, sodass sie in den Pflichthinweisen an den Betroffenen als (möglicher) Empfänger genannt werden müsste. Denn nach Art. 4 Nr. 9 DSGVO ist Empfänger eine „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle". Verschiedene Juristen argumentieren, dass das Wort „Stelle" eine gewisse Form der Selbstständigkeit mit sich bringt; so soll der Betriebsrat eine Stelle sein. Ungeachtet dessen variiert auch der Begriff der „Abteilung" von Unternehmen zu Unternehmen:

Es kann sich um ein „loses Gebilde" handeln oder um eine große Organisation innerhalb eines großen Unternehmens, die über Unterabteilungen (Stellen?) verfügt. Wenn nun eine Abteilung die „andere Stelle" ist, welche die Daten empfängt, müsste es aber auch die „eine Stelle" geben, welche die Daten weitergibt. Damit müsste eine „originär zuständige Stelle" im Unternehmen definiert werden, welche die Daten „eigentlich" erhebt, sodass von dieser aus alle anderen Abteilungen als „andere Stellen" erscheinen. Wenn nun aber die „originär zuständige Stelle", z. B. die Personalabteilung, die Daten im Einzelfall doch nicht erhebt, sondern z. B. das Empfangssekretariat die telefonisch durchgegebene Religionszugehörigkeit

des neuen Mitarbeiters schnell notiert, würde dann die Personalabteilung dadurch zur „empfangenden Stelle“? Man kann also nur darauf vertrauen und hoffen, dass der Begriff „Stelle“ nicht zu weit ausgelegt wird.

Das österreichische Bundesverwaltungsgericht hat sich dazu in einer Entscheidung vom 10. Dezember 2018 im Zusammenhang mit der Marketing- und der Vertriebsabteilung einer Bank auf den Grundsatz, dass Mitarbeiter keine „Empfänger“ sein können, berufen und dann aber einschränkend ausgeführt:

„Gegenständlich geht es um die Frage, ob die Werbe- und Marketingabteilung und die Abteilung „XXXX Costumer Experience Management“ als „andere Aufgabengebiete“ der Beschwerdegegnerin angesehen werden müssen und damit unter den Empfängerbegriff fallen würden, der eine Pflicht zur Beauskunftung nach Art. 15 Abs. 1 lit. c DSGVO nach sich ziehen würde. Dies wird vom erkennenden Senat verneint: den Erläuterungen der Beschwerdegegnerin vom XXXX.2017 und den Schlussfolgerungen der belangten Behörde ist dahingehend zu folgen, dass diese beiden Tätigkeitsgebiete der Beschwerdegegnerin nicht als ausreichend eigenständig und „anders“ wahrzunehmen sind, sondern Unterstützungsleistungen oder „akzessorische“ Leistungen zum Kerngeschäft – Bankwesen – darstellen.“

Das klingt nach einer weiteren „Grauzone“: Hiernach müsste die Sachnähe einzelner Sub-Organisationen innerhalb einer größeren Organisation beurteilt werden, und erst ab einer bestimmten (welchen?) „Sachferne“ ist die andere Abteilung als „Empfänger“ anzugeben. Die Nachricht lautet also (wieder einmal): Einfacher wird’s auch mit Rechtsprechung nicht.

Fall 7:
Wann liegt Auftragsverarbeitung vor, wann nicht?

Praktischer Fall: Die Lohnbuchhaltung eines Unternehmens wird an einen Steuerberater ausgelagert, der aber für das Unternehmen zugleich Steuererklärungen erstellt und einreicht.

Alternativ: Die Personalverwaltung eines Tochterunternehmens wird an eine zentrale Abteilung der Konzernmutter ausgelagert und in diesem Rahmen werden einzelne Fälle auch arbeitsrechtlich begutachtet.

Wo Auftragsverarbeitung aufhört und der Status als Verantwortlicher anfängt, war in den Grenzbereichen auch schon unter „altem Recht" nie eindeutig – dasselbe gilt übrigens auch für die Abgrenzung zu mehreren „gemeinsam Verantwortlichen" (dazu unten Fall 16). Der Fall, in dem zwei Verantwortliche Daten einander übermitteln, weil ein Unternehmen bestimmte Tätigkeiten outgesourct hat, wurde früher als „Funktionsverlagerung" von der Auftragsverarbeitung abgegrenzt, wobei es diesen Begriff allerdings im Bundesdatenschutzgesetz selbst nie gab. Die Aufsichtsbehörden behelfen sich seit jeher mit Listen „typischer" Auftragsverarbeitungstätigkeiten und „typischer" Fälle, in denen der Verarbeitende der Verantwortliche ist. Dabei ist es wichtig zu beachten, dass, würde kein Fall der Auftragsverarbeitung vorliegen, aber dennoch eine Auftragsverarbeitungsvereinbarung abgeschlossen worden sein, keine wesentlichen datenschutzrechtlichen Probleme entstehen würden. Aber der Auftragnehmer wäre nun einmal hinsichtlich der Datenverarbeitung strikt weisungsunterworfen, was eventuell mit seinem Selbstverständnis (als Freiberufler), mit dem einschlägigen Berufsrecht (Aufbewahrungspflichten etc.) oder mit anderen Anforderungen nicht zu vereinbaren ist. Der umgekehrte Fall, dass jemand Auftragsverarbeiter ist, aber keine Auftragsverarbeitungsvereinbarung abgeschlossen hat, ist datenschutzrechtlich wesentlich problematischer. Der letztgenannte Fall führt nämlich auf jeden Fall zu einem Problem des verantwortlichen „Auftraggebers", die Vorgaben des Art. 28 DSGVO verletzt zu haben, aber auch – zumindest wenn kein Legitimationsgrund für eine Übermittlung vorliegt – zu einem Problem des Auftragsverarbeiters, der aber kein solcher sein will/soll (s. dazu auch unten Fall 27).

➢ Keine eigene Legitimationsgrundlage für die Weitergabe notwendig

Der wesentliche Grund, warum man eine Auftragsverarbeitungssituation zielgerichtet anstreben würde, ist, dass zumindest nach landläufiger Ansicht für die Weitergabe von Daten an

einen weisungsgebundenen Auftragsverarbeiter keine datenschutzrechtliche Legitimationsgrundlage erforderlich ist. Verantwortlicher und Auftragsverarbeiter werden als eine Art Einheit angesehen und der Datenaustausch zwischen ihnen ist zumeist unproblematisch möglich. Allerdings gibt es – wie bei jeder Einzelfrage innerhalb der DSGVO – auch hierzu abweichende Ansichten. Entsprechend wird argumentiert, dass die Weitergabe von personenbezogenen Daten an einen Auftragsverarbeiter „natürlich" einen Verarbeitungsvorgang darstellt, zu dem „natürlich" eine Legitimationsgrundlage gegeben sein muss. In der Praxis sei das meist Art. 6 Abs. 1 S. 1 lit. f) DSGVO. Dann würde sich aber in jedem einzelnen Fall der Auftragsverarbeitung – neben der Interessenabwägung als solcher – die Frage stellen, ob die Datenweitergabe an den Auftragsverarbeiter (und damit die Auftragsverarbeitung selbst) „erforderlich" ist, und außerdem hätte der Betroffene auch noch ein Widerspruchsrecht gegen die Auftragsverarbeitung (Art. 21 Abs. 1 DSGVO). Wenn aber an die Verarbeitung durch einen datenschutzrechtlich weisungsgebundenen Auftragsverarbeiter dieselben Legitimationsanforderungen gestellt werden wie an die Übermittlung an sonstige Dritte, dann wäre kaum zu erklären, warum bzw. wofür es das Institut der Auftragsverarbeitung überhaupt gibt. Nur um dem Verantwortlichen „einfach so" noch mehr Pflichten (Art. 28 Abs. 1 DSGVO) aufzuerlegen?

Der Thüringer Landesbeauftragte für Datenschutz knüpft dagegen in seinem Tätigkeitsbericht 2018 die datenschutzrechtliche Legitimation der Verarbeitungshandlungen des Auftragsverarbeiters an die Legitimation des Verantwortlichen an:

„Für die Weitergabe von personenbezogenen Daten an den Auftragsverarbeiter und die Verarbeitung durch den Auftragsverarbeiter bedarf es insofern keiner weiteren gesetzlichen Rechtsgrundlage im Sinne des Art. 6 bis 10 der DS-GVO als derjenigen, auf die der Verantwortliche seine Verarbeitung stützt."

Das bedeutet allerdings im Umkehrschluss, dass wenn der Verantwortliche die Daten nicht rechtmäßig verarbeitet, der Auftragsverarbeiter diese auch nicht rechtmäßig verarbeiten kann. Nun kann aber der Auftragsverarbeiter in aller Regel gar nicht selbst prüfen, ob der Verantwortliche über eine taugliche datenschutzrechtliche Legitimationsgrundlage verfügt, da er verschiedene Aspekte der Verarbeitung – etwa die Erhebung und den weiteren Kontext – oft nicht kennt. Es wäre daher interessant zu sehen, wie ein Verantwortlicher reagiert, wenn ihm der Auftragsverarbeiter ins Stammbuch – sprich: in die Auftragsverarbeitungsvereinbarung – schreibt, dass der Verantwortliche das Bestehen einer datenschutzrechtlichen Legitimationsgrundlage versichert.

➢ Wie wird Auftragsverarbeitung definiert?

Datenschutzbehörden neigen traditionell dazu, Auftragsverarbeitungen dort anzunehmen, wo der Auftragnehmer mechanische datenverarbeitende Tätigkeiten im Sinne einer weisungsgebundenen „verlängerten" Werkbank ausführt. Eine Tätigkeit „ohne eigenen Wertungs- und Entscheidungsspielraum" forderten auch die Gerichte unter dem – allerdings etwas anders formulierten – vormaligen Bundesdatenschutzgesetz. Neben diesem eingeschränkten „Freiheitsgrad" des Beauftragten wird häufig weiter angenommen, dass die Datenverarbeitung als solche den Gegenstand der Auftragstätigkeit bilden müsse. Auftragstätigkeiten, die über die reine Datenverarbeitung hinausgehen, können also dazu führen, dass nicht mehr von einer „Auftragsdatenverarbeitung" (als eigenständigem „Vertragstyp") gesprochen werden kann. Das bayerische Landesamt für Datenschutzaufsicht führt in seinem Tätigkeitsbericht 2017/2018 dazu aus:

„Auftragsverarbeitung im datenschutzrechtlichen Sinne liegt nach unserer Auffassung nur in Fällen vor, in denen eine Stelle von einer anderen Stelle im Schwerpunkt mit der Verarbeitung personenbezogener Daten beauftragt wird. Die Beauftragung mit fachlichen Dienstleistungen anderer Art, d. h. mit Dienstleistungen, bei denen nicht die Datenverarbeitung im Vordergrund steht bzw. bei denen die Datenverarbeitung nicht zumindest einen wichtigen (Kern-)Bestandteil ausmacht, stellt unserer Meinung nach keine Auftragsverarbeitung im datenschutzrechtlichen Sinne dar".

Hiernach würde etwa das Waschen von Arbeitskleidung mit aufgesticktem Namen keine Auftragsverarbeitung sein, denn der Vertragsgegenstand ist das Waschen, nicht die Verarbeitung von Daten. Auch das Ausdrucken von Fotos an einem Automaten in einem Drogeriemarkt dürfte danach keine Auftragsverarbeitung sein, denn der Vertragsgegenstand ist nicht die Erhebung von Fotos mit erkennbaren Personen (wie bei der Kameraüberwachung), sondern das Drucken von Fotos. In einem Urteil vom September 2019 hat das Amtsgericht Mannheim diese Sichtweise im Grundsatz bestätigt, als es annahm, dass der Verwalter einer Wohnungseigentümergemeinschaft nicht lediglich eine „datenverarbeitende Hilfsfunktion" erbringt und daher kein Auftragsverarbeiter sein könne. Aber lässt sich diese Trennlinie so dem Gesetz entnehmen oder ist diese Interpretation einfach nur „vernünftig"?

Art. 28 Abs. 1 DSGVO beginnt mit den Worten „Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen" – heißt das nun, dass der Auftrag auf die reine (Daten-) „Verarbeitung" beschränkt sein muss oder kann die (Auftrags-) Datenverarbeitung auch nur irgendein Teil eines allgemeineren Auftrags sein? Im erstgenannten Fall wäre der Anwendungsbereich der Auftragsverarbeitung tatsächlich stark beschränkt. Hinzu kommt, dass schon die Definition

von „Verarbeitung“ als „Vorgang im Zusammenhang mit personenbezogenen Daten“ sehr vage ist, da hiernach die personenbezogene Daten nicht zwangsläufig das eigentliche Objekt des Vorgangs sein müssen, sondern es nur irgendeinen Zusammenhang zwischen Vorgang und personenbezogenen Daten geben muss. Der „Vorgang“ kann also eigentlich auch ganz andere Informationen als personenbezogenen Daten zum Gegenstand haben. Weil das alles nicht so einfach ist, behalfen sich die Aufsichtsbehörden in der Vergangenheit mit Katalogen. Bestimmte (plakative) Beispielsfälle sind danach Auftragsverarbeitung, andere nicht.

Demgegenüber haben Vertreter der Wirtschaft den Anwendungsbereich bereits 2013 viel weiter gezogen. Eine Auftragsdatenverarbeitung konnte danach auch dann vorliegen, wenn dem Auftragnehmer weitgehende, auch über die reine Unterstützung bei der Datenverarbeitung hinausgehende Aufgaben übertragen werden. Maßgeblich sollte nur sein, dass der Auftraggeber die volle Verantwortung für die gesamte Datenverarbeitung beim Dienstleister übernimmt und der Auftragnehmer keine eigenen Entscheidungen trifft (diese aber vorbereiten darf). Diese Auffassung wird auch unter der DSGVO weiter vertreten: Danach darf es durchaus auch große „weisungsfreie Räume“ (also Eigenverantwortlichkeit) des Beauftragten geben, ohne dass eine Auftragsverarbeitung ausscheidet. Schließlich heißt es auch in Art. 28 Abs. 1 DSGVO nur „Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen“ – und ein „Auftrag“ (im Wortsinne) muss nicht in jedem Aspekt strikt weisungsgebunden oder auf die Verarbeitung personenbezogener Daten beschränkt sein. Dann wäre der Anwendungsbereich der Auftragsverarbeitung immens.

Es gibt daher viele Fälle, in denen unklar ist, ob nun Auftragsverarbeitung begrifflich vorliegt oder nicht. Als Beispiel kann die Administration von Reisebuchungen der Beschäftigten eines Unternehmens durch ein beauftragtes Reisebüro dienen. Das kann eine „beratungsintensive“ Tätigkeit sein oder einfach nur die Zurverfügungstellung einer entsprechenden IT-Plattform. Wo die Grenze liegt, ist schwer abzuschätzen. Das Problem liegt nun aber gerade darin, dass die Grenze durch Vertrag selbst nicht „definierbar“ ist, wie das bayerische Landesamt für Datenschutzaufsicht in seinem Tätigkeitsbericht 2017/2018 festhält (obwohl doch die Frage, ob eine Verarbeitung im Auftrag eines Verantwortlichen erfolgt, gerade ein bestimmtes Vertragsverhältnis voraussetzt):

„Für die Frage, ob ein Verhältnis über eine Auftragsverarbeitung vorliegt, kommt es nicht auf die vertraglichen Vereinbarungen der Parteien an, sondern auf die tatsächlichen Abläufe der Datenverarbeitung.“

Wie schwierig eine inhaltlich „richtige“ Definition ist, zeigt auch die Diskussion um Software-Wartungsverträge, die auch als Auftragsverarbeitungsverhältnisse angesehen werden, obwohl es dort nicht um eine zielgerichtete Verarbeitung der Daten, sondern (nur) um ein „in-Berührung-kommen“ mit personenbezogenen Daten geht (s. u. Fall 27).

➢ Der Schulfall: Steuerberater

Ein „typischer“ Fall der eigenständigen Verantwortlichkeit ist nach traditioneller Auffassung die Einschaltung eines Berufsgeheimnisträgers, denn dieser erbringt als Angehöriger eines freien Berufs höherwertige Dienstleistungen (Wirtschaftsprüfung, Steuerberatung, Rechtsberatung), die über reine (mechanische) Datenverarbeitung weit hinausgehen. Allerdings hat davon abweichend der Bundesgerichtshof in einem Urteil aus dem Jahr 2016 (zum vormaligen Bundesdatenschutzgesetz) auch einen Arzt schon zum Auftragsverarbeiter „degradiert“. Ein „typischer“ Fall der Auftragsverarbeitung hingegen ist die Auslagerung der Lohnbuchhaltung in ein Rechenzentrum, Stichwort DATEV. Was aber, wenn ein Steuerberater beauftragt wird, (ausschließlich) die Lohnbuchhaltung zu übernehmen? Eigentlich kann es keinen Unterschied zur DATEV geben; die Tätigkeit ist dieselbe. Wenn der Steuerberater wie im eingangs dargestellten Fall aber auch Steuererklärungen erstellt, also als Freiberufler in Anspruch genommen wird, zählt dann der Schwerpunkt der Tätigkeit? Oder führt das Erstellen der Steuererklärungen dazu, dass das Verhältnis als Ganzes in eine eigene Verantwortlichenstellung „umschlägt“? Oder kann die datenschutzrechtliche Stellung des Steuerberaters „gesplittet“ werden, wie das Verwaltungsgericht Bayreuth in der oben genannten Entscheidung vom Mai 2018 angedeutet hat?

Anhand einer dazu veröffentlichten Äußerung des bayerischen Landesamts für Datenschutzaufsicht lässt sich erahnen, wie Aufsichtsbehörden mit dem Thema umgehen (werden). Kurz gesagt ist die Aufsichtsbehörde der Ansicht, Steuerberater unterlägen keinen Weisungen ihrer Mandanten. Die Behörde führt aus:

„Bei Steuerberatern ist nach unserer Auffassung zu sehen, dass diese nach dem insoweit geltenden Fachrecht (Steuerberatungsgesetz) als Freiberufler selbständig, weisungsunabhängig und eigenverantwortlich tätig sind und dementsprechend auch einer strafbewehrten persönlichen Geheimhaltungspflicht unterliegen (vgl. z. B. § 57 Steuerberatungsgesetz, § 203 Abs. 1 Nr. 3 des Strafgesetzbuches). Das widerspricht der Weisungsgebundenheit im Sinne von Art. 28 Abs. 3 lit. a DS-GVO. Des Weiteren ist den Steuerberatern eine gewerbliche Tätigkeit außerhalb des Steuerberaterrechts grundsätzlich untersagt (§ 57 Abs. 4 Nr. 1 Steuerberatungsgesetz).

Auch wenn Steuerberater nur die Lohnbuchhaltung für einen Mandanten durchführen, müssen sie dafür aufgrund des Steuerberaterrechts die eigene Verantwortung übernehmen und können sich nicht, wie allgemeine Dienstleister zur Lohnabrechnung, auf Weisungen von Mandanten berufen.

Steuerberater arbeiten deshalb aus unserer Sicht regelmäßig eigenverantwortlich aufgrund eines Mandantenvertrags und dürfen von den Mandanten im Rahmen der Erforderlichkeit für ihre Tätigkeit im Sinne von Art. 6 Abs. 1 Satz 1 lit. f DS-GVO personenbezogene Kunden- und/oder Arbeitnehmerdaten verarbeiten.“

Die bayerische Aufsichtsbehörde – Aufsichtsbehörden anderer Bundesländer sehen dies anders – geht also davon aus, dass eine außerhalb des Datenschutzrechts weisungsungebundene Tätigkeit keine datenschutzrechtliche Auftragsverarbeitung darstellt und dass der Steuerberater weisungsfrei tätig ist. Das berücksichtigt jedoch nicht, dass Weisungsgebundenheit ein Graukeil und keine schwarz/weiß-Frage ist. Meist sind Auftragsverhältnisse – wie auch Steuerberaterverträge – zivilrechtlich sog. Geschäftsbesorgungsverträge, für die das BGB u. a. auf § 665 BGB verweist, der davon handelt, dass der Beauftragte unter bestimmten Bedingungen „von den Weisungen des Auftraggebers“ abweichen darf. Und natürlich muss der Steuerberater „Anweisungen“ des Mandanten beachten (bzw. darf sich darauf berufen), diese Anweisungen dokumentieren und, wenn diese rechtswidrig sein sollten, das Mandatsverhältnis kündigen. Der Steuerberater handelt also innerhalb der erteilten Anweisungen (Rahmen) eigenverantwortlich (Ausfüllung) und muss überdies Anweisungen des Mandanten – das hat der Bundesgerichtshof oft entschieden – aus seiner berufsrechtlichen Perspektive hinterfragen und auf Probleme hinweisen. Aber das bedeutet nicht, dass der Steuerberater „weisungsfrei“ handelt. Und wenn man sich den Wortlaut der DSGVO vergegenwärtigt (s. o.), liegt bei der Beauftragung eines Steuerberaters sicherlich begrifflich ein „Auftrag“ vor.

Wenn also die mit der Letztentscheidungskompetenz ausgestatteten Gerichte nicht irgendwann das Dogma aufstellen, dass ein „Auftrag“ eben ein „Auftrag“ ist, gleich wo er sich auf der „Weisungsgebundenheitsskala“ einordnet, dann wird aus der Menge möglicher „Aufträge“ vermutlich immer nur eine Teilmenge eine Auftragsverarbeitung im Sinne der DSGVO darstellen. Und wo die Grenze genau liegt, muss kein Gericht entscheiden, weil es nur über den konkreten Fall entscheidet. So kann einstweilen jeder seine Menge definieren, wie er das für richtig hält, weil der EU-Gesetzgeber es vorgezogen hat, derartige Details der Meinungspluralität der Praxis zu überlassen.

Bemerkenswert ist, dass sich ausgerechnet zur Frage der Einordnung von Steuerberater-Verträgen eine Initiative im (deutschen) Bundesrat zu einer gesetzlichen Klarstellung auf deutscher Ebene gebildet hat. Als gäbe es nicht wichtigere Baustellen, um grundlegende Dinge innerhalb der DSGVO klarzustellen. Aber ganz grundsätzlich stellt sich bei diesem Ansinnen natürlich die Frage, was der deutsche Gesetzgeber – abseits der von der DSGVO ausdrücklich vorgesehenen Öffnungsklauseln – überhaupt regeln darf. Die Verbindlichkeit der hier angestrebten „EU-Auslegungs-Gesetze" auf nationaler Ebene könnte dann wieder nur der Europäische Gerichtshof verbindlich beurteilen, dessen Entscheidungstendenz als europäisches Gericht bekannt sein dürfte.

➢ Exkurs: Die externe Verarbeitung von Beschäftigtendaten

Aus dem letzten Absatz der Stellungnahme der Bayerischen Aufsichtsbehörde wird übrigens noch eine weitere „Baustelle" deutlich: Die Aufsichtsbehörde geht davon aus, dass personenbezogene Daten von Arbeitnehmern des Mandanten wie auch personenbezogene Daten von Kunden des Mandanten – wohl solchen, die natürliche Personen sind – vom Steuerberater aufgrund einer Interessenabwägung (Art. 6 Abs. 1 S. 1 lit. f) DSGVO) verarbeitet werden. Der Steuerberater hat also ein berechtigtes Interesse, die Daten zu verarbeiten, welches das Interesse des Arbeitnehmers oder Kunden überwiegt, dass dessen Daten nicht vom Steuerberater ihres Arbeitgebers bzw. Lieferanten verarbeitet werden. Da aber das Interesse des Steuerberaters – als „outgesourcte" Steuer- bzw. Lohnbuchhaltungsabteilung – nur ein vom Interesse seines Mandanten selbst abgeleitetes Interesse ist, stellt sich die Frage, ob nicht die Legitimationsgrundlagen, welche die Datenverarbeitung beim Mandanten selbst „tragen", auch die Datenverarbeitung durch den Steuerberater legitimieren. Oben in Fall 1 wurde dies für die unternehmensbezogenen Kontaktdaten des Beschäftigten und deren Verarbeitung durch dritte Unternehmen thematisiert, hier geht es nun um Stammdaten des Beschäftigten bzw. sogar um „Personalaktendaten". Die „Kontakt-/Werbedaten" des Beschäftigten werden noch unten in Fall 22 thematisiert.

Dieser Gedanke würde unabhängig davon gelten, ob eine Auftragsverarbeitungssituation vorliegt oder eine Übermittlung an einen anderen (selbstständigen) Verantwortlichen. Rechtsgrundlage für die Verarbeitung von Arbeitnehmerdaten ist § 26 BDSG. Dass nur der Arbeitgeber sich auf diese Rechtsgrundlage berufen darf, steht nicht im Gesetz, wird aber von Juristen wie selbstverständlich so „hineingelesen". Solange die Verarbeitung der personenbezogenen Daten „für Zwecke des Beschäftigungsverhältnisses verarbeitet werden", was bei der Lohnbuchhaltung der Fall ist, müsste § 26 BDSG eigentlich auch die weitere Verarbeitung durch den Steuerberater legitimieren können. Schon die Übermittlung an den Steu-

erberater ist für die Durchführung des Beschäftigungsverhältnisses (Lohnabrechnung) „erforderlich“, wenn sich der Arbeitgeber entscheidet, diese Funktion an den Steuerberater „outzusourcen“, und dasselbe gilt für die Verarbeitung beim Steuerberater. Das könnte sogar für die Übermittlung an eine zentral in den USA betriebene HR-Abteilung eines US-Konzern mit Tochtergesellschaften in der EU gelten – oder ist das für die Durchführung des Beschäftigungsverhältnisses nicht „erforderlich“ (§ 26 Abs. 1 S. 1 BDSG) und dem US-Konzern der Aufbau einer eigenen HR-Abteilung in der EU „zumutbar“?

Für die Verarbeitung der personenbezogenen Daten des Kunden, mit dem der Mandant des Steuerberaters einen (Liefer-) Vertrag geschlossen hat, gilt hingegen Art. 6 Abs. 1 S. 1 lit. b) DSGVO. Auch hier muss die Datenverarbeitung nur zur Erfüllung eines Vertrags mit dem Betroffenen „erforderlich“ sein – es ist nicht notwendig, dass dieser Vertrag gerade mit dem Verantwortlichen besteht. Sofern also die Datenverarbeitung durch den Steuerberater im Rahmen der Buchhaltung für die Vertragserfüllung „erforderlich“ ist, müsste sich auch der Steuerberater hierauf berufen können.

Diese Sichtweise – der Steuerberater „teilt“ die Legitimationsgrundlage seines Mandanten, die dieser gegenüber dem Betroffenen geltend machen kann – vertritt, wie oben zitiert, der Thüringer Landesbeauftragte für Datenschutz im Fall der Auftragsverarbeitung. Ob diese Sichtweise auch auf Datenübermittlungen an (selbstständig) Verantwortliche übertragen werden kann, ist offen. Es ist aber nicht unwichtig: Kann der Steuerberater sich „nur“ auf eine Interessenabwägung berufen, so könnte der Betroffene der Verarbeitung widersprechen (Art. 21 DSGVO). In der Praxis würde dies eine Menge (Prüf-)Arbeit auslösen bis hin zur Einschränkung der Verarbeitung (Art. 18 DSGVO). Kann sich der Steuerberater auch – neben dem ursprünglichen Verantwortlichen – auf die Legitimationsgrundlage (Anstellungs-)Vertrag berufen, besteht diese Möglichkeit des Betroffenen nicht.

Es wird also noch in vielen Fallgestaltungen viele Diskussionen über die „richtige“ datenschutzrechtliche Legitimationsgrundlage geben. Und wenn man die Entscheidung des Bundesgerichtshofs vom Juli 2018 in Sachen Facebook-Account liest, könnte es sogar viele Fälle von „beides ist richtig“ geben (s. dazu u. Fall 8), was allerdings nur solange nützlich ist, wie die Konsequenzen der unterschiedlichen Legitimationsgrundlagen nicht auseinanderlaufen.

Fall 8:
Wie lange „hält“ die Interessenabwägung beim Direktmarketing?

Praktischer Fall: Die Huber AG betreibt eine CRM-Datenbank mit Kontaktdaten von Ansprechpartnern. Teils handelt es sich um Repräsentanten von Unternehmen, mit denen die Huber AG in Geschäftsbeziehung stand, steht oder gerne stehen würde. Teils handelt es sich um soziale oder politische Kontakte, etwa der Vertreter von Vereinen, die von der Huber AG gesponsert werden, oder von Personen des öffentlichen Lebens, mit denen die Huber AG den Kontakt pflegt. Solche Kontaktdaten ergeben sich aus E-Mail-Verkehren, aus der Übergabe von Visitenkarten, aus Telefonaten und Ähnlichem. Die Huber AG geht davon aus, aufgrund ihres Interesses an Direktmarketing (hierzu zählt nicht nur kommerzielle Kommunikation im engeren Sinne, d. h. Werbung) die entsprechenden Daten aufgrund einer Interessenabwägung verarbeiten zu dürfen.

EU-Kommissarin Věra Jourová erklärte im Mai 2018 in einem Interview: „Wenn Ihnen jemand eine E-Mail schreibt und Ihnen zugesteht, dass Sie seine Daten verwenden dürfen, dann ist doch klar, dass er Ihnen eine Einwilligung erteilt.“ Dabei bezog sie sich wohl darauf, dass die DSGVO im Regelfall (Art. 4 Nr. 11 DSGVO) keine „ausdrückliche“ Einwilligung fordert, sondern auch eine stillschweigende Einwilligung zulässig ist, solange eine „eindeutige bestätigende Handlung“ des Betroffenen vorliegt. Damit bedürfte es in solchen Fällen – dazu wird man auch die Übergabe einer Visitenkarte zählen – keiner Interessenabwägung. Auch die „Orientierungshilfe“ der Datenschutzkonferenz zum Thema Direktwerbung vom November 2018 führt aus, dass die Übergabe einer Visitenkarte grundsätzlich eine wirksame Einwilligung („zur Informationszusendung oder weiteren geschäftlichen Kontaktaufnahme“) darstellt.

- Welche Informationen setzt die Erteilung einer Einwilligung voraus?

Erwägungsgrund 42 der DSGVO sieht aber verschiedene Mindestinformationen vor, die dem Einwilligenden bekannt sein müssen, bevor er eine „informierte“ Einwilligung abgeben kann (*„Damit sie in Kenntnis der Sachlage ihre Einwilligung geben kann, sollte die betroffene Person mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen.*“). Bezüglich der Konkretisierung der Zwecke fordert die Datenschutzkonferenz übrigens selbst, dass „die Produkte oder Dienstleistungen, für die geworben werden soll“, dem Einwilligenden bekannt sein müssen, ansonsten

ist seine Einwilligung nicht „informiert“ genug, um wirksam sein zu können. Jeder Unternehmer weiß nun aber, dass ein „Kontakt“ eben oft zunächst nur ein „Kontakt“ ist; an welchem Produkt oder an welcher Dienstleistung der „Kontakt“ später einmal interessiert sein könnte, weiß man häufig anfangs noch nicht. Dabei muss man noch nicht einmal an einen Mischkonzern, der ein breites Produktportfolio abdeckt, denken.

Daneben verlangt Art. 7 Abs. 3 DSGVO, dass die betroffene Person vor Abgabe der Einwilligungserklärung davon in Kenntnis gesetzt werden muss, dass sie das Recht hat, ihre Einwilligung jederzeit zu widerrufen, und dass durch diesen Widerruf die Rechtmäßigkeit der bis dahin erfolgten Verarbeitung nicht berührt wird.

Mitunter werden auch noch weitergehende Informationen im Vorfeld der Einwilligung gefordert. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg vertritt im Ratgeber Beschäftigtendatenschutz vom März 2019 etwa die Auffassung, dass die Kenntnis der Speicherdauer notwendige Voraussetzung für eine wirksame Einwilligung sei. Der Thüringer Landesbeauftragte für Datenschutz geht hingegen in seinem Tätigkeitsbericht 2018 aufs Ganze und fordert für eine informierte Einwilligungserklärung das „gesamte Paket“ der Pflichtinformationen – und zusätzlich die Pflichtinformationen als solche:

„Als Orientierungsrahmen für Art und Umfang der Informationspflichten gelten die Angaben in Art. 13 und 14 der DS-GVO. Diese Informationspflichten sind jedoch zusätzlich zu erfüllen [...].“

In die gleiche Richtung weist übrigens die „Planet49“-Entscheidung des Europäischen Gerichtshofs vom Oktober 2019, die aber genaugenommen nicht im Datenschutzrecht, sondern im „E-Privacy-Recht“ spielt (s. dazu auch noch unten Fall 17 in Bezug auf die Speicherung von Cookies an sich). Dort geht es um eine Vorschrift für Cookies auf Endgeräten – gleich ob personenbezogen oder nicht –, nach der eine Einwilligung des Nutzers „auf der Grundlage von klaren und umfassenden Informationen“ erforderlich ist, die er vorher gemäß der (damals gültigen) Datenschutz-Richtlinie zu erhalten hat. Der Verweis in der sog. „Cookie-Richtlinie“ von 2009 auf die Datenschutz-Richtlinie 1995 wird seit Inkrafttreten der DSGVO durch einen Verweis auf Art. 13/14 DSGVO ersetzt. Hier fordert der Europäische Gerichtshof aber auch für die Zeit vor dem Inkrafttreten der DSGVO nicht nur sämtliche in der Datenschutz-Richtlinie 1995 vorgeschriebenen Pflichtinformationen als Voraussetzung für die wirksame „Cookie-Einwilligung“, sondern auch die Angabe der Dauer der Verarbeitung (die heute standardmäßig in Art. 13/14 Abs. 2 lit. a DSGVO vorgegeben ist). In der Datenschutz-Richtlinie 1995 war nämlich der Katalog der Pflichtinformationen noch mit

„insbesondere“ eingeleitet worden und die Dauer der Verarbeitung war nicht ausdrücklich mit aufgeführt worden – der Europäische Gerichtshof hat die Dauer der Verarbeitung hier als weitere Pflichtinformation „hinzu-interpretiert“ (wobei der Europäische Gerichtshof die „Dauer der Speicherung des Cookies“ insoweit mit der „Dauer der Verarbeitung“ gleichsetzt). Dieses „insbesondere“ fehlt in Art. 13/14 DSGVO, d. h. der dort genannte Katalog der Pflichtinformationen ist abschließend (bis jemandem etwas Neues dazu einfällt). Man findet sich also durchaus in guter Gesellschaft, wenn man fordert, dass dem Betroffenen vor einer Einwilligung zunächst sämtliche Pflichtinformationen zur Verfügung gestellt werden müssen; vorher ist keine wirksame Einwilligung möglich.

Wenig konkret ist hingegen das Standard-Datenschutzmodell in Abschnitt B2 („Einwilligungsmanagement“). Hiernach ist die Einwilligung nur wirksam, wenn vorher eine *„umfassende Information des Betroffenen über die Datenverarbeitung erfolgt ist“*. Was „umfassend“ genau meint, wird nicht definiert.

Ausnahmen von diesen „Vorinformationspflichten“, wie weit auch immer diese gezogen werden mögen, sieht der Wortlaut der DSGVO nicht vor, obgleich manche Juristen – Jourová folgend – es bei einer stillschweigend erteilen Einwilligung damit nicht so genau nehmen. Die „durch die Umstände“ erteilte Einwilligung, die nach dieser Auffassung trotz des klaren Wortlauts doch (vom Ergebnis her) „irgendwie möglich sein muss“, erinnert insoweit an die eigentlich vom Wortlaut her ebenso unbedingte Forderung der DSGVO, die Pflichthinweise „zum Zeitpunkt der Erhebung“ mitzuteilen, gleich ob die Erhebung schriftlich, mündlich, telefonisch oder durch Handzeichen erfolgt. Auch der Weg über die dem Betroffenen „offensichtlich“ bereits vorliegenden Pflichtinformationen (Art. 13 Abs. 4, 14 Abs. 5 lit. a) DSGVO) ist nur schwer zu begründen (s. oben Fall 1).

➢ Ist eine Interessenabwägung die bessere Einwilligung?

Eine Passage des Tätigkeitsberichts 2017/2018 des bayerischen Landesamtes für Datenschutzaufsicht in Bezug auf Nutzeranfragen in einem Kontaktformular – als Analogie zur E-Mail – legt nahe, dass dort die Ansicht der EU-Kommissarin über das Vorliegen einer Einwilligung nicht geteilt wird:

„Grundsätzlich bedarf es keiner Einwilligung durch den Nutzer, da die Datenverarbeitung auf eine Interessenabwägung nach Art. 6 Abs. 1 Buchstabe f DS-GVO gestützt werden kann. Der Verantwortliche hat ein berechtigtes Interesse daran, Nutzeranfragen, die über das Kontaktformular eingehen, zu beantworten.“

Kann man sich aber nun nicht sicher sein, dass die Übersendung einer E-Mail oder die Übergabe einer Visitenkarte, wenn letzteres als „Erhebung" einzustufen wäre (siehe oben Fall 1), eine (stillschweigende) Einwilligung darstellt, so neigen Juristen dazu, eine Alternativbegründung hinterherzuschieben. Man würde „hilfsweise", also für den Fall, dass die Einwilligung nicht „funktioniert hat", von einer Interessenabwägung ausgehen. Ein Unwirksamkeitsrisiko kann es ja nicht nur im Hinblick auf die „Nichtausdrücklichkeit" der Einwilligung oder auf die nicht ausreichende Vorinformationen, sondern auch im Hinblick auf eine Einwilligungserklärung mit zu weit gefasster Zweckdefinition geben (im Extremfall: „Einwilligung in die Verarbeitung zu beliebigen Zwecken").

Allerdings gibt es nun wieder Juristen, die in Anlehnung an das (deutsche) Recht der Allgemeinen Geschäftsbedingungen eine solche Hilfskonstruktion für unzulässig halten. Hiernach war entweder der Legitimationsgrund das, was der Verantwortliche in den Pflichthinweisen angegeben hat, oder er war etwas anderes, dann hat der Verantwortliche den falschen Legitimationsgrund angegeben und (u. a.) falsche Pflichthinweise gegeben (s. auch u. Fall 26). Auf Basis dieses Gedankens hat die österreichische Datenschutzbehörde in einem Bescheid vom November 2018 ausgeführt:

„Zunächst ist der Einwilligung nicht mit der erforderlichen Klarheit zu entnehmen, für welche Datenverarbeitungen die Einwilligung die Rechtsgrundlage darstellt. In der bereitgestellten Information nach Art. 13 DSGVO wird als Rechtsgrundlage zwar die Einwilligung genannt, es werden jedoch auch andere Rechtsgrundlagen, wie bspw. die Erfüllung rechtlicher Verpflichtungen oder die Wahrung berechtigter Interessen angeführt. Insofern ist unklar, für welche konkreten Datenverarbeitungen die Einwilligung die Rechtsgrundlage ist. Die Einwilligungserklärung erweist sich daher in diesem Punkt als rechtswidrig."

Dieser Gedanke ist durchaus ernst zu nehmen, denn nicht notwendige Einwilligungen können auch rechtsmissbräuchlich von ahnungslosen Kunden „eingeheimst" werden, wie folgende Passage aus dem Tätigkeitsbericht 2018 der Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen zeigt:

„Nach der Datenschutzgrundverordnung sind Datenverarbeitungen im Zusammenhang mit Vertragsabschlüssen oder aufgrund besonderer gesetzlicher Verpflichtungen grundsätzlich zulässig, ohne dass es einer gesonderten Einwilligung der oder des Betroffenen bedürfte. Wir erhielten Anhaltspunkte dafür, dass das eine oder andere Kreditinstitut die Unsicherheit seiner Kundinnen und Kunden über die neuen Datenschutzregeln dazu genutzt haben könnte,

sich unter Vorspiegelung der Notwendigkeit der Abgabe einer datenschutzrechtlichen Einwilligungserklärung weitergehende Möglichkeiten zur Auswertung und Nutzung der Kundendaten zu verschaffen. Mangels personeller Ressourcen konnten wir diesen Hinweisen bislang bedauerlicherweise nicht nachgehen."

Im zugrundeliegenden Gedankengang ähnlich formuliert der Landesdatenschutzbeauftragte von Mecklenburg-Vorpommern in seinem Tätigkeitsbericht 2018 zur „überflüssigen" Einwilligung:

„In vielen Fällen ist jedoch die Datenverarbeitung bereits aufgrund eines Vertrages durch eine andere Rechtsgrundlage (nämlich Art. 6 Abs. 1 b DS-GVO) abgedeckt. In derartigen Fällen wurden jedoch oft (um „sicherzugehen") zusätzliche Einwilligungen von den jeweiligen Vertragspartnern eingeholt. Dies kann bei diesen zu dem Missverständnis führen, man könne die erteilten Einwilligungen mit Wirkung für die Zukunft widerrufen, wodurch die wirksame Rechtsgrundlage für eine Datenverarbeitung entfallen würde, obwohl eine solche in dem geschlossenen Vertrag nach Art. 6 Abs. 1 b DS-GVO tatsächlich existiert. Mit Blick auf den Grundsatz der Transparenz und Fairness gemäß Art. 5 Abs. 1 a DS-GVO ist jedoch ein Wechseln zwischen Einwilligungen und anderen Rechtsgrundlagen grundsätzlich unzulässig."

Dem liegt jeweils der Gedanke zugrunde, dass eine Einwilligung nur eingeholt werden „darf", wenn man als Betroffener auch die „echte" Wahl hat, die Einwilligung zu verweigern. Würde nämlich der Betroffene die Einwilligung verweigern und der Verantwortliche erwidern „Gut, dann machen wir es eben über eine Interessenabwägung", dann wirft das schon die Frage auf, ob der Verantwortliche überhaupt ernstlich eine Einwilligung einholen wollte.

Der Thüringer Landesbeauftragte für Datenschutz postuliert daher in seinem Tätigkeitsbericht 2018 letztlich – aus Fürsorge für den Verantwortlichen – ein Rangverhältnis der Legitimationsgrundlagen:

„Sofern die datenverarbeitende Stelle bei der betroffenen Person eine Einwilligungserklärung einholt, signalisiert sie ihr, dass es für die Zulässigkeit einer Datenverarbeitung allein auf ihr Einverständnis ankommen soll. Dann aber wäre es in sich widersprüchlich und damit unzulässig, wenn die datenverarbeitende Stelle im Falle der Verweigerung oder Unwirksamkeit der Einwilligung alternativ doch wieder auf einen gesetzlichen Erlaubnistatbestand zurückgreifen könnte [...]. Daher sollte die Einwilligung als Rechtsgrundlage für die Verarbeitung nur dann herangezogenen werden, wenn die Verarbeitung auf keinen der anderen

Sachverhalte in Art. 6 Abs. 1 Buchstabe b) bis f) DS-GVO gestützt werden kann. Zwar steht die Einwilligung als Rechtsgrundlage gleichwertig neben den anderen Erlaubnistatbeständen, ist aber als Rechtsgrundlage für eine Datenverarbeitung deutlich unzuverlässiger, da der jederzeit mögliche Widerruf der Einwilligungserklärung dazu führt, dass die betroffene Person die Löschung der sie betreffenden Daten verlangen kann und der Verantwortliche verpflichtet ist, diese Daten ohne unangemessene Verzögerung zu löschen."

Diese „Vorzugswürdigkeit" der Interessenabwägung aus pragmatischen Gründen könnte allerdings mit dem möglichen, unten in Fall 17 betrachteten Vorrang der Einwilligung kollidieren. Diese weitere Problematik soll daher hier nicht vertieft werden.

Angefügt sei hier lediglich noch, dass auch die griechische Datenschutzaufsichtsbehörde in die gleiche Richtung tendiert. Dort hatte ein Arbeitgeber „sicherheitshalber" Einwilligungen seiner Beschäftigten eingeholt:

„The principles of lawful, fair and transparent processing of personal data pursuant to Article 5(1)(a) of the GDPR require that consent be used as the legal basis in accordance with Article 6(1) of the GDPR only where the other legal bases do not apply so that once the initial choice has been made it is impossible to swap to a different legal basis. In case the data subject withdraws his or her consent, it is not allowed to carry on the processing of personal data under a different legal basis. Where the legal basis of consent is properly applied, in the sense that no other legal basis is applicable, refusal of consent or its withdrawal is equivalent to an absolute prohibition on the processing of personal data.

Consent of data subjects in the context of employment relations cannot be regarded as freely given due to the clear imbalance between the parties.

In this case, the choice of consent as the legal basis was inappropriate, as the processing of personal data was intended to carry out acts directly linked to the performance of employment contracts, compliance with a legal obligation to which the controller is subject and the smooth and effective operation of the company, as its legitimate interest."

Ohne dass es dort spezifisch um Pflichthinweise ging, hat allerdings zumindest der BGH in seiner Entscheidung zur Vererbung von Facebook-Accounts vom Juli 2018 ohne weiteren Kommentar eine bestimmte Datenverarbeitung legitimationsmäßig „auf zwei Beine gestellt", nämlich gleichberechtigt auf einen Vertrag und auf eine Interessenabwägung. Der BGH – wenn auch nicht der für Datenschutzrecht eigentlich zuständige Senat – schreibt wörtlich:

„Die Erlaubnistatbestände des Art. 6 Abs. 1 Buchst. b und f DS-GVO begründen jeweils eigenständig die datenschutzrechtliche Zulässigkeit der Zugangsgewährung für die Klägerin."

Das klingt so, als könnte man eine datenschutzrechtliche Legitimation auch alternativ begründen – darf das nun aber auch ein Verantwortlicher in seinen Pflichthinweisen (s. auch u. Fall 26) oder nur ein Gericht?

➢ Woraus werden mutmaßliche Interessen abgeleitet?

Beruft sich also die Huber AG von vornherein nur auf eine Interessenabwägung, so würde sie mit ihrem (im „gesetzesgleichen" Erwägungsgrund 47 als legitim bezeichneten) Interesse an Direktmarketing – in einem weit verstandenen Sinne – argumentieren. Weit verstanden deshalb, weil es durchaus auch den Standpunkt gibt, dass „Direktmarketing" im genannten Erwägungsgrund nicht die Ansprache neuer Kunden, sondern nur das Bewerben von Bestandskunden meint. Dieser Ansicht ist etwa die Niederländische Datenschutzaufsichtsbehörde in einer Veröffentlichung vom November 2019. Nach ihr kann Direktmarketing in Bezug auf Neukunden kein legitimes Interesse begründen, denn ein solches Interesse sei ein rein kommerzielles Interesse. Kommunikation mit Neukunden kann, wenn man dies zugrunde legt, nur auf Basis einer Einwilligung in die Bewerbung stattfinden.

Das Rechtsprinzip, das einer Interessenabwägung zugrunde liegt, kann als „mutmaßliche Einwilligung" des Betroffenen umschrieben werden. Man fragt also, ob der Betroffene, wenn er es objektiv und neutral sehen würde, mit der Datenverarbeitung einverstanden wäre, wenn ihm das Interesse des Verantwortlichen und sein eigenes Interesse bekannt wären und er diese beiden „fair" abwägen würde. Umgangssprachlich heißt Interessenabwägung schlicht „Na, da kann der Betroffene doch eigentlich nichts dagegen haben". Bei abstrakter Betrachtung (Abwägung) würde demnach meist das Direktmarketing-Interesse des Unternehmens an der Verarbeitung der Kontaktdaten das auf der anderen Seite stehende Interesse des Betroffenen, davon verschont zu bleiben, überwiegen. Insbesondere gilt dies natürlich, wenn der Betroffene ein Repräsentant eines Unternehmens ist und es nur um seine unternehmensbezogenen Kontaktdaten geht (s. dazu auch u. Fall 20). Die Berliner Beauftragte für Datenschutz und Information führt in ihrem Jahresbericht 2018 zur Abwägung sibyllinisch aus:

„Entscheidend ist daher, ob die Verarbeitung personenbezogener Daten für bestimmte Bereiche der Sozialsphäre typischerweise akzeptiert oder abgelehnt wird und ob es der Vernunft entspricht, Nachteile für das Selbstbestimmungsrecht hinzunehmen“.

Das birgt natürlich ein erhebliches Risiko, zu einem falschen Abwägungsergebnis zu gelangen, weil man „typische“ Verhaltensweisen in einer Sozialsphäre unterschätzt hat. Der „Drahtverhau“ der Interessenabwägung wird unten in Fall 29 eingehender behandelt.

- Nachlassende Interessen

Der im vorliegenden Fall entscheidende Aspekt betrifft nun jedoch die Frage, ob nach einer bestimmten Zeit, in der entweder die Kontaktdaten des Betroffenen von der Huber AG nicht verwendet werden oder der Betroffene nicht auf Kommunikationsversuche der Huber AG reagiert, diese Interessenabwägung „kippt“, weil das Direktmarketing-Interesse der Huber AG „verblasst“ ist. Diese Frage stellt sich für die Interessenabwägung übrigens ebenso wie für eine erteilte Einwilligung (wobei es hier nicht um Spezialfälle wie die Produkteinstellung eines Produktes, auf dessen Bewerbung sich die Interessenabwägung oder Einwilligung ursprünglich bezog, gehen soll).

Hinsichtlich dieses – durchaus nicht identischen – Parallelfalles ziehen die Aufsichtsbehörden in der „Orientierungshilfe“ der Datenschutzkonferenz zum Thema Direktwerbung vom November 2018 eine Entscheidung des Landgerichts München I aus dem Jahr 2010 in einem einstweiligen Verfügungsverfahren – also nach „summarischer Prüfung des Anspruchs“, d. h. mit reduziertem Prüfungsmaßstab – heran. Im zugrunde liegenden Fall hatte eine Privatperson eine Werbe-E-Mail erhalten und ein Wettbewerbsverein verlangte die Unterlassung solcher Zusendungen auf Basis des Wettbewerbsrechts. Der Absender der Werbe-E-Mail erklärte, die betroffene Person habe etwa 17 Monate vor der E-Mail-Zusendung an einem Gewinnspiel teilgenommen und sich dort einverstanden erklärt, Werbe-E-Mails zu erhalten. Der Betroffene bestritt dies, einen präsenten Zeugen des Absenders wollte das Gericht nicht anhören. Es urteilte vielmehr in wenigen Sätzen, dass es gar nicht darauf ankomme, ob die Einwilligung seinerzeit erteilt worden war, denn selbst wenn der Betroffene diese erteilt hätte, hätte sie „jedenfalls ihre Aktualität“ verloren. Das Gericht hat also eine Einwilligungserklärung im Sinne des Wettbewerbsrechts einem Verfallsdatum unterworfen. Weder ging es hier um Datenschutzrecht (um die DSGVO schon gar nicht) noch wurde die Frage beantwortet, wie ein solches Verfallsdatum zum Gesetzestext „hinzuerfunden“ werden kann – denn der Gesetzestext sieht ein solches Verfallsdatum nicht explizit vor. Dies hat übrigens der Bundesgerichtshof Anfang 2018 – mit Verweis auf ähnliche Urteile anderer Gerichte aus den Jahren 2008, 2011 und 2013 – klargestellt:

„Eine zeitliche Begrenzung einer einmal erteilten Einwilligung sieht weder die RL 2002/58/EG noch § 7 UWG vor. Hieraus ergibt sich, dass diese – ebenso wie eine Einwilligung nach § 183 BGB – grundsätzlich nicht allein durch Zeitablauf erlischt“.

Im Falle des BGH sah die geprüfte wettbewerbsrechtliche Einwilligungsklausel eine Wirkung der Einwilligung bis zwei Jahre nach dem Ende eines „Telekommunikationsdienstleistungsvertrages“ vor. Wie also die deutschen Datenschutzbehörden den Mut aufbringen können, sich auf die genannte „Mindermeinungs-Entscheidung“ des Landgerichts München I aus dem Jahr 2010 zu beziehen, bleibt im Dunkeln.

Für den Fall der Interessenabwägung wird man demnach allenfalls – im Einklang mit einigen Kommentaren, aber ohne Äußerung der Datenschutzbehörden spezifisch dazu – konstatieren müssen, dass die Zeitdauer für den Interessenfortfall nach den Umständen des Einzelfalles zu beurteilen ist. Eine klare Zeit(ober)grenze für den „Ablauf“ der Interessenabwägung – wenn es diesen denn überhaupt geben sollte – wird man aus der DSGVO hingegen nicht herleiten können. Allerdings ging der sog. „Düsseldorfer Kreis“ der Datenschutzbehörden unter dem zuvor geltenden BDSG noch mit Blick auf Kundendaten von einer festen Frist aus, nämlich davon, dass diese im Grundsatz zwei Jahre nach dem letzten aktiven Geschäftskontakt zu einer betroffenen Person für die werblichen Zwecke der Reaktivierung und Rückgewinnung genutzt werden können. Nach Ablauf dieser Frist sei somit regelmäßig von einer fehlenden Erforderlichkeit der Datenspeicherung auszugehen.

Ein Bußgeldbescheid der Berliner Beauftragten für Datenschutz vom September 2019 lässt den konkreten Maßstab nicht erkennen:

„Nach den Feststellungen der Berliner Datenschutzbeauftragten hatte die Delivery Hero Germany GmbH in zehn Fällen Konten ehemaliger Kundinnen und Kunden nicht gelöscht, obwohl die Betroffenen jahrelang – in einem Fall sogar seit dem Jahr 2008 – nicht mehr auf der Lieferdienst-Plattform des Unternehmens aktiv gewesen waren.“

Hier wird also der ungefähre Maßstab „jahrelang“ verwendet. Im Beschluss der Datenschutzkonferenz zum Thema Asset Deal vom Mai 2019 wird dies für die Übernahme von Bestandskunden auf drei Jahre festgeschrieben:

„Daten von Bestandskundinnen und -kunden, bei denen die letzte aktive Vertragsbeziehung mehr als 3 Jahre zurückliegt, unterliegen bei einer erwerbenden Stelle einer Einschränkung

der Verarbeitung. Diese Daten dürfen zwar übermittelt, aber eben nur wegen gesetzlicher Aufbewahrungsfristen genutzt werden.“

Auch hier bleibt völlig unklar, woher diese Frist kommt, die zwar der zivilrechtlichen Regelverjährung entsprechen mag, was aber mit Datenschutzrecht und Interessenabwägung – noch dazu ohne jede Begründung – wenig zu tun hat.

➢ Fristenmanagement oder Warten auf Widerspruch?

Den meisten Literaten und Richtern wird allerdings nicht klar sein, was das in der Praxis heraufbeschwört: Jedes Unternehmen müsste für jeden Kontakt eine „Eieruhr“ führen, die durch tatsächlichen Kontakt mit dem Betroffenen „neu aufgezogen“ wird. Ist die „Eieruhr“ einmal abgelaufen, kann die Interessenabwägung die weitere Verarbeitung dieser konkreten Kontaktadresse nicht mehr rechtfertigen; die Daten müssen dann gelöscht werden. Wie lange aber ist die Zeit, auf welche die „Eieruhr“, gegebenenfalls mehrmals, eingestellt wird? Dies ist ganz entscheidend für die Frage, wie lange die Speicherung (d. h. das Vorhalten) dieser Kontaktdaten noch rechtmäßig ist. Denn nach dieser Zeit endet der Lebenszyklus der entsprechenden Kontaktdaten aus datenschutzrechtlichen Gründen. Und dies ist – wie immer im Datenschutzrecht – eine Frage des Einzelfalls.

Man könnte nun allerdings auch einen Schritt weitergehen und die Interessenabwägung datenschutzrechtlich solange gültig sein lassen, bis die betroffene Person widerspricht (was sie jederzeit tun kann). Man würde also, um es im Sinne des Wettbewerbsrechts und der dortigen Regelungen über „unzumutbare Belästigungen“ auszudrücken, eine einzige „Belästigung“ der betroffenen Person in Kauf nehmen, aber den Zeitpunkt dieser „Belästigung“ dem Verantwortlichen überlassen. Nach der ersten Verwendung der Kontaktdaten – also der „Belästigung“ – kann die betroffene Person dann entscheiden, ob sie wieder (wann auch immer) belästigt werden will. Widerspricht sie, dürfen die Daten nicht mehr für Direktmarketing-Zwecke verwendet werden. Tut sie das nicht, darf sie noch einmal – gleich zu welchem Zeitpunkt – „belästigt“ werden. Warum soll das nach 12 oder 17 Monaten anders zu sehen sein als nach 8 oder 10 Jahren? Auch nach 17 Monaten wird die betroffene Person schon vergessen haben, dass sie ihre Daten für Direktmarketing-Zwecke zur Verfügung gestellt hat – so wohl auch im oben beschriebenen Fall des Landgerichts München I. Der Wortlaut der DSGVO schließt diese Lesart nicht aus.

Fall 9:
Ist das Schutzniveau der DSGVO verzichtsfähig?

Praktischer Fall: Siehe oben Fall 2: Frau Maier sendet der Huber AG eine (unverschlüsselte) E-Mail mit ihrer Bewerbung, welche neben einem Foto auch die Angabe enthält, dass Frau Maier zu 60 % schwerbehindert ist.

Alternativ: Der Mandant sendet dem Anwalt verschiedene Unterlagen zu einem anstehenden Klageverfahren per E-Mail, der Anwalt beantwortet dies mit einem Schriftsatzentwurf per E-Mail an den Mandanten. Gegebenenfalls hat der Mandant im Rahmen der Begründung des Mandatsverhältnisses eine Erklärung unterzeichnet, dass ihm die Gefahren unverschlüsselten E-Mail-Verkehrs bekannt sind, er aber trotz dieser Gefahren unverschlüsselt E-Mails mit seinem Anwalt austauschen möchte.

Möglicherweise wird die E-Mail zwischen den Servern automatisch transportverschlüsselt (wenn beide Server die sogenannte „TLS-Verschlüsselung" nutzen), möglicherweise wird die E-Mail auch unverschlüsselt gesendet. Für den Bediener (absendende/empfangende Person) ist das nur dann erkennbar, wenn diese Form der Verschlüsselung in den Servern als „mandatory" eingestellt wird. Denn nur in diesen Fällen wird die Übertragung vom sendenden Server abgelehnt, sodass der Absender eine „Fehlermeldung" erhält. Eine Ende-zu-Ende-Verschlüsselung ist hingegen ohne vorherigen Austausch von Schlüsseln bzw. Zertifikaten über eine „gewöhnliche" E-Mail-Adresse ohnehin technisch nicht möglich. Der Landesdatenschutzbeauftragte von Mecklenburg-Vorpommern führt in seinem Tätigkeitsbericht 2018 aus, die Ende-zu-Ende-Verschlüsselung sei der „Stand der Technik" (im Sinne von Art. 32 DSGVO), fügt aber an, es sei „in der Praxis in absehbarer Zeit noch immer nicht durchgängig möglich [...], eine Ende-zu-Ende-Verschlüsslung durchzusetzen", sodass auch eine Transportverschlüsselung (mit TLS 1.2, STARTTLS und DANE) „hinnehmbar" sei. Als Alternative wird das Versenden von verschlüsselten PDF- und ZIP-Dateien als E-Mail-Anhänge mit entsprechend „starkem" Passwort angeführt.

Der Landesdatenschutzbeauftragte Nordrhein-Westfalen führt auf seiner Internetseite unter dem Punkt „Technische Anforderungen an technische und organisatorische Maßnahmen beim E-Mail-Versand" aus:

„Die Kommunikation per E-Mail bedarf mindestens der Transport-Verschlüsselung, wie sie von den namhaften europäischen Providern standardmäßig angeboten wird.

Die Transportverschlüsselung sollte entsprechend der Technischen Richtlinie „BSI TR-03108 Sicherer E-Mail-Transport" implementiert sein. In Abhängigkeit vom Schutzbedarf der versendeten Daten und dem Risiko können Abweichungen von der Richtlinie statthaft sein.

Es ist zu berücksichtigen, dass bei einer Transportverschlüsselung die E-Mails auf den E-Mail-Servern im Klartext vorliegen und grundsätzlich einsehbar sind. Bei besonders schützenswerten Daten (z. B. Kontobewegungsdaten, Finanzierungsdaten, Daten zum Gesundheitszustand, Mandantendaten von Rechtsanwälten und Steuerberatern, Beschäftigtendaten) ist eine alleinige Transportverschlüsselung möglicherweise nicht ausreichend. Zusätzliche technische und organisatorische Maßnahmen, wie z. B. eine Ende-zu-Ende-Verschlüsselung können geboten sein. Sollte dies nicht gewährleistet werden können, sind ggf. alternative Übertragungswege denkbar: Hierzu zählen der elektronische Austausch über eine gesicherte Verbindung (Web-Portal des Verantwortlichen mit Zugangsbeschränkungen) oder die klassische postalische Zusendung.

Der Betreff der E-Mail sollte keine personenbezogenen Daten enthalten."

Die Huber AG könnte sich allerdings gleichwohl auf den Standpunkt stellen, es sei ja Sache von Frau Maier, ihre Bewerbung nicht per E-Mail zu verschicken. Sie habe damit auf den Schutz einer Verschlüsselung für ihre E-Mail verzichtet. Der Anwalt könnte sich auf den Standpunkt stellen, wenn der Mandant ihm schon unverschlüsselte E-Mails schickt, habe er doch freiwillig auf diesen Aspekt der Datensicherheit verzichtet. Dies gilt umso mehr, wenn der dies schriftlich erklärt.

Muss also die Huber AG eine besondere Plattform für Bewerber zur Verfügung stellen, sodass die Bewerber ihre Unterlagen über eine verschlüsselte Verbindung hochladen können? Es gibt Datenschutzaufsichtsbehörden, die in dieser Richtung der „notwendigen Optionen" bei den Übermittlungswegen tendieren. Das würde dann auf ein Bewerberportal mit einem eigenem „Datenbereich" für jeden Bewerber hinauslaufen, dann aber bitte mit entsprechenden Zugangsdaten: Die französische Datenschutzaufsichtsbehörde CNIL hat im Mai 2019 ein Bußgeld von EUR 400.000 für ein Unternehmen verhängt, innerhalb von dessen Webauftritt sämtliche Daten von Mietwohnungsbewerbern einfach unter X.com/Zahl.pdf abrufbar waren, d. h. man konnte „irgendeine" Zahl eingeben und erhielt „irgendein Dokument" von „irgendeinem Betroffenen" zurück. Und muss der Anwalt dem Mandanten die Verwendung einer Ende-zu-Ende-Verschlüsselung von E-Mails aufoktroyieren und anderenfalls auf E-Mail-Kommunikation verzichten, auch wenn der Mandant darauf beharrt und weiter unverschlüsselte E-Mails schreibt? Oder darf der Anwalt darauf vertrauen, dass ein Mandant bei

seinem Server die Verwendung einer TLS-Verschlüsselung vorgegeben hat, oder muss er das eigens prüfen? Muss der Anwalt einen elektronischen Datenraum mit gesichertem Zugriff für den Mandanten bereitstellen für den Fall, dass der Mandant E-Mail-Kommunikation nicht verschlüsseln kann oder will?

- Kann der Betroffene auf Datensicherheit verzichten?

Soweit das in der Vergangenheit überhaupt thematisiert wurde, sind Aufsichtsbehörden der Ansicht, dass die DSGVO durchgängig zwingendes Recht ist. Auch und insbesondere die Schutzvorschriften der DSGVO in Sachen Datensicherheit (Art. 32 Abs. 1 lit. a DSGVO) stünden nicht zur Disposition der Parteien. In diesem Sinne entschied auch die österreichische Datenschutzbehörde im November 2018. Ein Betroffener könne nicht auf den Schutz verzichten, den die DSGVO ihm gewährt. Es ist offen, was das konkret für den Beispielsfall der Verschlüsselung bedeutet, d. h. welches Vorgehen hier später als „Stand der Technik", als „hinsichtlich der Implementierungskosten zumutbar", als „dem Risiko angemessen" angesehen werden wird, das auch mit Zustimmung des Betroffenen nicht unterschritten werden durfte. Die DSGVO sagt dazu nichts.

Im Grundsatz könnte man sagen: Natürlich kann der Betroffene verzichten, denn er kann ja selbst eine unverschlüsselte E-Mail verschicken oder auch gleich die Information bei Facebook oder Twitter öffentlich zugänglich machen. Man würde ihm aber von vornherein keinen Vorwurf machen können, „seine" Daten nicht gemäß den Anforderungen des Art. 32 DSGVO verschlüsselt zu haben – denn er ist der Betroffene, nicht der Verantwortliche. Er kann als Betroffener auch eine Information des Verantwortlichen, die nur seine personenbezogenen Daten enthält, öffentlich machen (soweit er keine sonstigen Gesetze verletzt), denn er hat die Verfügungsbefugnis über „seine" personenbezogenen Daten. Für die Frage aber, ob der Betroffene den Verantwortlichen von dessen sicherheitsbezogenen Pflichten „entlasten" kann, ergibt sich daraus eigentlich nichts, denn das hängt davon ab, ob diese Pflichten des Verantwortlichen nur zugunsten des Betroffenen bestehen oder die Einhaltung dieser Pflichten auch im Interesse der „Allgemeinheit" liegt (im Sinne von „Gesetze sind einzuhalten").

- Standesrecht der Rechtsanwälte

Die berufsständischen Vertretungen (Bundessteuerberaterkammer etc.) sind der Meinung, dass ein – so müsste man es wohl zusammenfassen – „einigermaßen wohlinformierter" Betroffener freiwillig auf den Schutz der Verschlüsselung verzichten könne. Die Rechtsanwaltszunft hat dazu ab 2020 Folgendes in ihr Standesrecht aufgenommen (§ 2 BORA):

„Zwischen Rechtsanwalt und Mandant ist die Nutzung eines elektronischen oder sonstigen Kommunikationsweges, der mit Risiken für die Vertraulichkeit dieser Kommunikation verbunden ist, jedenfalls dann erlaubt, wenn der Mandant ihr zustimmt. Von einer Zustimmung ist auszugehen, wenn der Mandant diesen Kommunikationsweg vorschlägt oder beginnt und ihn, nachdem der Rechtsanwalt zumindest pauschal und ohne technische Details auf die Risiken hingewiesen hat, fortsetzt."

Dahinter steht die (schon wesentlich länger als der Datenschutz bestehende) Vorstellung, dass (alleine) der Mandant „Herr des Geheimnisses" ist. Dies lässt sich allerdings mit einem „zwingenden Datenschutz", der nicht zur Disposition der Parteien steht, nicht vereinbaren – schon gar nicht in Bezug auf Dritte, deren Daten erfahrungsgemäß in der Mehrzahl der Kommunikationen ebenfalls verarbeitet werden (man denke nur an das cc-Feld in E-Mails oder Mailtexte, die inhaltlich Bezug zu dritten Personen aufweisen). Deshalb bestimmt das Standesrecht denn auch ergänzend: *„Die Vorschriften zum Schutz personenbezogener Daten bleiben unberührt"*. Und auch die Zustimmung des Bundesjustizministeriums zur neuen Regelung enthielt die Warnung, diese sei formal auf das anwaltliche Berufsrecht beschränkt. Einerseits ist damit erklärtermaßen gemeint, dass der Anwalt auch bei Zustimmung des Mandanten in eine bestimmte Kommunikationsform bei seiner Antwort die nach dem Datenschutzrecht erforderlichen Schutzmaßnahmen ergreifen muss. Damit sollen vor allem die Schutzstandards der IT-Sicherheit (Art. 32 DSGVO) gemeint sein, was im Bereich des E-Mail-Versands – neben allgemeiner Serversicherheit wie Virenschutz, Firewall, Betriebssystems-Updates etc. – eigentlich nur eine TLS-Verschlüsselung oder eine (Passwort-)Verschlüsselung von Anlagen meinen kann. Andererseits lässt auch das Bundesjustizministerium offen, ob unverschlüsselte E-Mails unter der DSGVO überhaupt zulässig sind. Der Europäische Gerichtshof wird derartige (standesrechtliche) Regelungen bei einem DSGVO-Streitfall vermutlich weitgehend ignorieren. Die entscheidende Frage in diesem Kontext ist ohnehin: Muss der Anwalt, der seinen E-Mail-Server so konfiguriert hat, dass standardmäßig TLS-Verschlüsselung eingesetzt wird, dafür sorgen, dass der Server nicht (automatisch) unverschlüsselt E-Mails austauscht, wenn die „Gegenstelle" (also der E-Mail-Server des Kommunikationspartners) nicht ebenso konfiguriert ist? Dann würde bei Versendung einer E-Mail eine Fehlermeldung generiert und der Anwalt müsste dafür sorgen, dass der Kommunikationspartner entweder eine entsprechende Verschlüsselung „einschaltet" oder es müsste ein anderer Übertragungsweg – etwa über einen verschlüsselten Anhang – gewählt werden. Herkömmlich ist es anders, wie man einem Computermagazin entnehmen kann:

„Die SMTP-Clients in gängigen Mailservern sind grundsätzlich bedingungslos auf Transport eingestellt. Sie führen „Opportunistische TLS" durch. Bietet der Server STARTTLS an, versuchen sie verschlüsselten Transport herbeizuführen. Fehlt ESMTP im Banner des Servers, schalten sie auf herkömmliches SMTP zurück. Sie verzichten auf Transportverschlüsselung, weil es keine Gelegenheit (lat.: opportunitas) dazu gibt."

Nach einer Google-Statistik erfolgt zwischen 90 und 95% des E-Mail-Verkehrs unter TLS-Verschlüsselung, wobei sich dies auf sämtliche – auch veraltete und damit anfällige – TLS-Versionen erstreckt. Der Prozentsatz der Fälle, in denen die oben zitierte Technische Richtlinie „BSI TR-03108 Sicherer E-Mail-Transport" eingehalten wird, dürfte daher wesentlich darunter liegen. Und dass überhaupt bisher schon so viel E-Mail-Verkehr TLS-verschlüsselt wird, liegt mutmaßlich auch nicht an den DSGVO-Vorgaben, sondern daran, dass, wie ein US-Blog aufzählt, viele US-Compliance-Vorgaben – natürlich unabhängig von der DSGVO – (irgend)eine E-Mail-Verschlüsselung unbedingt erfordern:

„email encryption is a requirement for pretty much every compliance framework including HIPAA, HITECH, PCI DSS, Sarbanes-Oxley, GLBA, SB1386, SEC 17a-4, NASD3010, FRCP, FINRA, etc."

Das bayerische Landesamt für Datenschutzaufsicht vertritt im Kontext von Patientendaten eine etwas andere Lösung als das übliche schwarz/weiß zur Einwilligungsfähigkeit. Einwilligungen zur Absenkung des Schutzniveaus sollen zwar möglich, aber nicht grenzenlos sein:

„In keinem Fall ist ein völliges Absenken des Schutzniveaus möglich: Es gibt einen Mindeststandard (derzeit opportunistische Transportverschlüsselung), der eingehalten werden muss. Zudem muss eine dem Risiko der Rechte und Freiheiten entsprechende sichere Alternative ohne Medienbruch angeboten werden. Dies kann z. B. ein ausreichend sicheres Onlineportal oder ein inhaltsverschlüsselter E-Mail-Verkehr sein."

Ist das Risiko jedoch erhöht und die Anzahl der Kommunikationspartner begrenzt, so soll hiernach eine verpflichtende Transportverschlüsselung einzusetzen sein, soweit dies nicht im Einzelfall unverhältnismäßig ist. Gleichwohl fügt das bayerische Landesamt an:

„Eine Absenkung des Schutzniveaus sehen wir innerhalb sehr enger Grenzen nur dann als möglich an, wenn die betroffene Person damit einen Nutzen verbindet – „Komfort" würden wir selbstverständlich auch dazu zählen. Allerdings muss dann die Zustimmung für diese Form der E-Mail-Kommunikation eingeholt, die Risiken transparent beschrieben und eine

sichere Alternative ohne Medienbruch angeboten werden. Dies wäre beispielsweise dann der Fall, wenn ein Arzt oder eine Versicherung eine sichere Alternative mittels PGP oder einem Online-Portal bieten, ein Patient oder Kunde aber für sich entscheidet, nur mittels „normaler" E-Mail (d. h. opportunistisch transportverschlüsselt) kommunizieren zu wollen. Eine Absenkung unter einer Transportverschlüsselung sehen wir nicht als möglich an, da die Risiken massiv zunehmen würden und eine transparente Zustimmung für die meisten Betroffenen in Anbetracht der Komplexität des weltweiten Internetverkehrs samt Bedrohungsszenarien kaum einzuholen wäre. Eine sichere Alternative zur E-Mail könnte auch der Einsatz eines datenschutzkonformen Messengers oder ein mit Blick auf Sicherheit entwickeltes Online-Portal mit Zwei-Faktor-Authentifizierung sein."

➢ Schadensersatzansprüche

In einer Fallkonstellation, über die das Amtsgerichts Bochum im März 2019 entschied, hatte ein betreuter, d. h. nicht mehr selbst geschäftsfähiger, Betroffener, eine Anwältin als Betreuerin zugeordnet bekommen. Diese sendete sowohl die sie legitimierende „Bestallungsurkunde" als auch – nach dem Ende der Betreuung – den entsprechenden Nachweis über das Betreuungsende per unverschlüsselter E-Mail an den Vermieter des Betroffenen. Es ist nicht überliefert, ob die E-Mail TLS-verschlüsselt worden war oder nicht, also ob sie tatsächlich gänzlich „unverschlüsselt" war. Der Betroffene verlangte Schadensersatz.

Das Amtsgericht Bochum stellte zunächst fest, dass es kein Problem mit der datenschutzrechtlichen Legitimationsgrundlage für die Übermittlungen gebe, sondern nur ein Problem der Datensicherheit. Da allerdings nicht aufgezeigt werden konnte, dass ein (unbefugter) Dritter tatsächlich auf die übermittelten Daten zugegriffen hatte, wurde ein Schadensersatzanspruch gegen die Anwältin (Art. 82 DSGVO) verneint. Dies ist deshalb bemerkenswert, weil sowohl der Sicherheitsmangel als solcher (Art. 32 DSGVO) als auch eine „Bereitstellung" gegenüber (unbefugten) Dritten (s. dazu unten Fall 41) einen Datenschutzverstoß darstellt. Aber, so das Amtsgericht Bochum, ohne (irgendeinen) Schaden kein Schadensersatz. Darin steckt die Erkenntnis, dass alleine die Tatsache, dass Daten Dritten zugänglich waren, aber kein Zugriff nachweisbar ist, auch keinen immateriellen Schaden zur Folge hat. Das „Offen-Zutage-Liegen" von Daten würde demnach zwar ein Bußgeld auslösen können, wäre aber „schadensersatzfrei". Man wird sehen, ob sich dies als Grundsatz durchsetzt.

Fall 10:
Übermittlung in Drittländer: Beispiel Unternehmens-kontakte

Praktischer Fall: Die Dow Inc. mit Sitz in den USA möchte Aktien an der Huber AG erwerben. Im Rahmen der Transaktion wird eine Unternehmensprüfung (Due Diligence) bei der Huber AG durchgeführt und zu diesem Zweck eine Liste erstellt, wer bei der Huber AG für welches Thema im Rahmen der Due Diligence als Ansprechpartner fungiert (Umwelt, IT, Produktion, Controlling, Steuern etc.). Die Liste, welche die Namen, E-Mail-Adressen, Telefonnummern bei der Huber AG und die jeweiligen Mobiltelefonnummern enthält, wird der Dow Inc. und ihren Beratern zur Verfügung gestellt.

Das Thema Übermittlung personenbezogener Daten in Drittländer ist komplex. Die Erfahrungen mit dem „Safe Harbour"-Abkommen und die neuerlichen Diskussionen um das „Privacy Shield" zeigen, dass nachhaltige Rechtssicherheit in diesem Bereich bislang Luxus ist. Darüber hinaus ist in der Praxis einer globalisierten Wirtschaft, im Beispielsfall in Bezug auf internationale M&A-Transaktionen, den Beteiligten oft unklar, dass sie damit eine Übermittlung personenbezogener Daten in ein Drittland vornehmen.

Aber das Thema geht weit über M&A-Transaktionen oder sonstige individuelle Unternehmenskontakte hinaus: Jedes personenbezogene Datum – auch unternehmensbezogene Kontaktdaten der Mitarbeiter –, das auf einer Website weltweit abrufbar ist, wird weltweit zur Verfügung gestellt und damit selbstverständlich (auch) in Drittländer übermittelt, wenn jemand die Website aufruft. In derartigen Fällen wird bisweilen auf die „Lindqvist"-Entscheidung des Europäischen Gerichtshofs aus dem Jahr 2003 verwiesen, d. h. maßgeblich war wiederum die EU-Datenschutzrichtlinie aus dem Jahr 1995. Damals wurde derjenige, der die personenbezogenen Daten auf die Website „stellte" – genauer gesagt: der die Daten an den Hoster der Website übermittelte, der dann wiederum die Website zum Abruf bereithielt –, nicht als „Übermittler" dieser Daten eingestuft. Die zweite Stufe, also auf welcher Grundlage dann der Website-Hoster – im B2B-Bereich häufig das verantwortliche Unternehmen selbst – die Daten auch an Drittländer übermittelt, wurde dabei ausdrücklich nicht weiter betrachtet (denn „beklagt" war im Fall des Europäischen Gerichtshofs nicht der Website-Hoster selbst). Der Europäische Gerichtshof argumentierte insoweit gerade noch so eben, dass der Gesetzgeber wohl 1995 nicht die Internetnutzung als „Drittlandsübermittlung" einstufen wollte, denn damit würden ja die Sonderregelungen über die Drittlandsübermittlung generell für den Normalfall der Internet-Übermittlung gelten. Es kann also nicht sein, was

nicht sein darf: Der Abruf aus einem Drittland, das über kein der EU angemessenes Datenschutzniveau verfügt, würde so sämtliche Internetangebote „illegal" werden lassen. Eine hervorragende Argumentation in kritischen Situationen: Das kann der Gesetzgeber nicht gewollt haben. Wenn man auch bei der DSGVO immer so leicht argumentieren könnte wie der Europäische Gerichthof...

Wie dieses Urteil nach dem Inkrafttreten der DSGVO zu „lesen" ist bzw. ob ihm überhaupt noch irgendeine Bedeutung zukommt, ist völlig unklar. Im Sachverhalt der Entscheidung von 2003 hatte kein Abruf aus einem Drittland stattgefunden, d. h. es ging alleine um die „Abrufbarkeit" (und auch das eigentlich nicht, weil der Europäische Gerichtshof explizit nur über die Frage des „Hochladens", nicht über die Frage des „Herunterladens" zu entscheiden hatte). Wenn nun die personenbezogenen Daten aber zielgerichtet für den „weltweiten Abruf" zur Verfügung gestellt werden, sieht die Sache unter der DSGVO wohl anders aus. In diesem Zusammenhang wird bislang – soweit das Problem überhaupt erkannt wird – argumentiert, dass das „Verbreiten" durch eine Website keine „Übermittlung" darstelle, weil Art. 4 Nr. 2 DSGVO von „Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung" spricht, d. h. Verbreitung und Übermittlung sind nicht identisch, sondern unterschiedliche (Unter-)Fälle der Offenlegung. Die nur auf die Regulierung der „Übermittlung" in Drittländer abzielenden Regelungen der DSGVO (Art. 44 bis 50 DSGVO, s. dazu auch noch u. Fall 24) würden also auf ein „Verbreiten" in Drittländer keine Anwendung finden. Bei technischer Sichtweise allerdings werden die zu einer Website gehörenden (HTML- und sonstigen) Dateien vom Client-Browser des Seitenbesuchers zielgerichtet beim jeweiligen Webserver angefragt und an diesen „Punkt-zu-Punkt" (von IP-Adresse zu IP-Adresse) übermittelt (s. auch o. Fall 1). Welche Sichtweise hier am Ende zum Tragen kommen wird, ist eine Frage der Granularität (s. dazu noch u. Fall 14).

Doch zurück zum Fall. Geht man davon aus, dass die Dow Inc. nicht innerhalb des „Privacy Shield"-Mechanismus registriert ist und – weil es „nur" um die Anbahnung eines Aktienkaufs und Kontaktdaten von zuständigen Mitarbeitern geht – auch keine EU-Standardklauseln vereinbart werden sollen, bleibt eigentlich nur der Fall der besonderen ausdrücklichen Einwilligung der betroffenen Person (Art. 49 Abs. 1 lit. a DSGVO). Dies setzt voraus, dass die Mitarbeiter der Huber AG, die auf der Liste geführt werden, vor der Einwilligung *„über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurden"*. Mit anderen Worten: Die betroffene Person soll besonders gewarnt werden, dass ihre personenbezogenen Daten nun datenschutzrechtlich sicheren EU-Boden verlassen. Über welche Risiken genau aufzuklären ist, ist unklar. Sinngemäß wird der Satz zumindest etwa heißen „Es

besteht das Risiko, dass diese Daten in den USA zweckwidrig verwendet oder weitergegeben werden, ohne dass Sie dies erfahren oder dagegen vorgehen können". Allerdings fordern die Datenschutzbehörden in diesem Zusammenhang, dass der Betroffene darüber aufgeklärt wird, wohin genau nun seine Daten im Drittland gehen.

Das mag im Beispielsfall noch einigermaßen klar darstellbar sein, aber wenn das weltweite Zurverfügungstellen personenbezogener Daten auf einer Website zu einer „Übermittlung" führt, wird eine pauschale Einwilligung hierzu nach dieser Forderung der Aufsichtsbehörden zur Transparenz unmöglich zu erteilen sein. Im Übrigen wären die (anvisierten) Empfänger nicht nur im Rahmen der Pflichtinformationen, sondern auch (in der Rückschau) im Rahmen des Auskunftsanspruchs mitzuteilen. Müssten also, um einen Auskunftsanspruch gegenüber dem Betroffenen, dessen Daten im Internet (z. B. auf der Unternehmenswebseite) weltweit zur Verfügung gestellt wurden, erfüllen zu können, die IP-Adressen (oder Betreiber) sämtlicher Webseitenbesucher geloggt werden, weil auch diese „Empfänger" sind? Nach Art. 4 Nr. 9 DSGVO ist Empfänger jeder, dem personenbezogene Daten „offengelegt" werden, und die Offenlegung ist in Art. 4 Nr. 2 DSGVO als eine Form der Bereitstellung definiert.

Zurück zum Ausgangsfall: Es ist offen, ob ein Arbeitnehmer unter den aufgeführten Umständen eine „freiwillige" Einwilligung im Sinne von Art. 49 Abs. 1 lit. a DSGVO erteilen kann. Die Voraussetzungen, unter denen ein Arbeitnehmer eine freiwillige Einwilligung erteilen kann, sind schon bei „normalen" Verarbeitungshandlungen eher hoch (§ 26 Abs. 2 BDSG). Kann man bei einer Übermittlung in die USA davon sprechen, dass „Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen"? Immerhin spielen die Ansprechpartner der Huber AG keine leitende Rolle bei einer internationalen Transaktion, sondern sollen „passiv" als Ansprechpartner fungieren. Und was, das darf nicht vergessen werden, für die Praxis noch wichtiger ist: Wenn ein Arbeitnehmer seine Einwilligung verweigert – was jedenfalls möglich ist, Freiwilligkeit hin oder her –, platzt dann die Transaktion?

Fall 11:
Die Crux mit den „Verarbeitungsvorgängen“

Praktischer Fall: Die Huber AG erarbeitet ihr Verarbeitungsverzeichnis (Art. 30 DSGVO). Wie jedes Unternehmen verarbeitet sie Personaldaten der bei ihr beschäftigten Mitarbeiter. Wie viele „Verarbeitungstätigkeiten“ umfasst nun die Verarbeitung von Personaldaten?

Ebenso wie bei der Beschreibung technischer und organisatorischer Maßnahmen stellt sich beim Verarbeitungsverzeichnis die Frage des Detaillierungsgrades. Das Bayerische Landesamt für Datenschutzaufsicht hat in seiner Publikation „Erste Hilfe zur DSGVO“ in einem beispielhaft ausgefüllten Eintrag des Verarbeitungsverzeichnisses eine Verarbeitungstätigkeit als „Personalverwaltung“ bezeichnet. Ein Beispiel der Rechtsanwaltskammer München listet hingegen unter der Überschrift „Mitarbeiter“ die (Teil-)Prozesse „Personalakte“, „Zeiterfassung“, „Geburtstagsliste“, „Lohnbuchhaltung“ und „Schulungen“ auf. Aus der Praxis sind Fälle bekannt, in denen alleine die Personalabteilung im Rahmen ihrer datenschutzrechtlichen Bestandsaufnahme zu mehreren hundert Verarbeitungsvorgängen gelangte. Und wenn man sogar in jedem Löschvorgang einen eigenen Verarbeitungsvorgang sehen wollte, würde beim Einsatz eines Löschkonzepts jede Datenkategorie und Löschfrist zu einem eigenen Vorgang führen.

Letztlich geht es auch hier um ein Problem der Granularität (siehe dazu Fall 14). Man kann die DSGVO aus der „Vogelflugperspektive“ erfüllen, dann wird ein übliches mittelständisches Unternehmen nicht viel mehr als die Verarbeitungstätigkeiten Bewerberprozess, Personalverwaltung, Vorhalten der Ansprechpartner von Dienstleistern, Lieferanten und Behörden sowie Kundendatenverwaltung aufweisen. Man kann jede Verarbeitungstätigkeit aber auch wesentlich granularer aufgliedern. Welcher Maßstab der richtige ist, ergibt sich aus der DSGVO nicht. Mittelbar kann man schließen, dass anhand der Kategorien betroffener Personen und/oder der Kategorien der personenbezogenen Daten gegliedert werden soll – aber auch der Begriff „Kategorie“ ist ebenso interpretationsfähig. Hier wäre es wünschenswert gewesen, wenn der Gesetzgeber zumindest Beispiele für Verarbeitungstätigkeiten geliefert hätte. Ob das, was Aufsichtsbehörden dazu als „Guidance“ herausgeben, der DSGVO entspricht – die Aufsichtsbehörden sind, was bisweilen vergessen wird, nicht der Gesetzgeber –, wird sich zeigen.

Dasselbe Problem stellt sich übrigens auch bei anderen Anforderungen an das Verarbeitungsverzeichnis, beispielsweise welchen Abstraktionsgrad eine „allgemeine Beschreibung der technischen und organisatorischen Maßnahmen“ aufweisen muss.

Fall 12:
Die Datenkette

Praktischer Fall: Die Huber AG wurde von einer freiberuflichen Übersetzerin, Frau Schmidt, angeschrieben, die anbot, Übersetzungsdienstleistungen zu erbringen. Die Huber AG hat die Daten von Frau Schmidt daher in ihre Kontaktdatenbank übernommen und ihr Pflichthinweise nach der DSGVO zukommen lassen. Einige Zeit später erhielt die Huber AG ein Schreiben von Frau Schmidt, die mitteilte, sie sei nicht mehr als freiberufliche Übersetzerin tätig und die Huber AG möge bitte sämtliche personenbezogenen Daten über sie löschen. Dieses Schreiben gelangte bei der Huber AG nicht an die zuständige Stelle; die Daten wurden nicht gelöscht. Einige Zeit später fragt eine Tochtergesellschaft der Huber AG, die Müller GmbH, an, ob die Huber AG einen Übersetzer benennen könne. Die Huber AG gibt die Daten von Frau Schmidt an die Müller GmbH weiter.

Dieser Fall steht für ein Problem, das in Zukunft noch deutlicher zutage treten dürfte: Die Datenkette. Der Zivilrechtler fühlt sich an Besitz- und Eigentumsketten erinnert, an gutgläubigen Erwerb, Rechtsscheintatbestände und Abhandenkommen, der Strafrechtler an Hehlerei. Im Datenschutzrecht gilt jedenfalls: Jeder in einer Verarbeitungskette ist im Grundsatz voll verantwortlich für das, was in der Kette passiert (Art. 82 Abs. 2 DSGVO). Wurden Daten rechtswidrig nicht gelöscht oder übermittelt, haftet der Empfänger für diese Umstände im Grundsatz ebenso. Man muss also zwischen rechtmäßig erhobenen und übermittelten Daten einerseits und „toxischen" Daten andererseits unterscheiden.

Es ist nun vor diesem Hintergrund aber völlig unklar, welche Prüfpflichten der Empfänger hat, d. h. welche Formen von „due diligence" er hinsichtlich der Herkunft und Legitimationsgrundlage der Daten betreiben muss. Nur wenn der Empfänger nachweisen kann, dass *„er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist"* (Art. 82 Abs. 3 DSGVO), kann er sich entlasten. Welcher Aufwand dafür notwendig oder zumutbar ist (bzw. ob es Grenzen hinsichtlich dieses Aufwands gibt), erläutert das Gesetz nicht. Wie kann man also einen solchen Nachweis führen?

Der Vertragsrechtler würde sofort an Mängelgewährleistung oder Garantien denken: Die Müller GmbH müsste einen Datenübermittlungsvertrag mit der Huber AG abschließen und sich in diesem Vertrag garantieren lassen, dass die Daten rechtmäßig erhoben wurden, nicht gelöscht werden mussten und eine Legitimationsgrundlage für die Übermittlung vorliegt. Sicherheitshalber könnte die Müller GmbH im Vorfeld des Abschlusses dieses Vertrags ver-

langen, dass ihr die Einwilligung von Frau Schmidt vorgelegt wird – eine Interessenabwägung ist mit Wertungsrisiken behaftet – und die Huber AG garantiert, dass die Einwilligung nicht widerrufen wurde.

Aber neben dieser Problematik auf Empfängerseite geht es auch aufseiten des Übermittelnden noch weiter: Wenn Frau Schmidt ihren Widerrufsbrief nicht geschrieben hätte, sondern stattdessen bereits von Anfang an darum gebeten hätte, die Daten nicht an konzernfremde Dritte weiterzugeben, und die Müller GmbH als Empfängerin der Daten den Kontakt an einen Lieferanten der Müller GmbH weitergegeben hätte, dann wäre die Huber AG hierfür mitverantwortlich. Mit anderen Worten: Die Huber AG musste sicherstellen, dass sämtliche Informationen über die Bedingungen der weiteren Verarbeitung von ihr an die Müller GmbH weitergegeben und dort beachtet werden. Nur dann ist eine Enthaftung der Huber AG denkbar. Auch hier mag man wieder an vertragliche Verpflichtungen der Müller GmbH denken – das muss ja nicht eine notarielle Vereinbarung sein, es wäre auch ein einfacher E-Mail-Verkehr zwischen der Huber AG und der Müller AG bei Weitergabe der Daten über die Konditionen der Verwendung denkbar.

Die dargestellten Fallkonstellationen zeigen deutlich, dass „Datenschutz-Management“ nicht nur eine Worthülse ist. Nach der Vorstellung der DSGVO hat ein Verantwortlicher zu jedem Zeitpunkt vollen Überblick darüber, welche Daten er hat, wie und wie lange er diese verwenden und an wen er sie weitergeben darf, wie er eine rechtmäßige Herkunft sichergestellt hat und eine rechtmäßige weitere Verwendung sicherstellen wird und so fort. In einem perfekten System könnten personenbezogene Daten gar nicht „das Haus verlassen“, ohne dass automatisiert sichergestellt wird, dass sich der Empfänger verpflichtet, die Daten im Rahmen des Zwecks zu verarbeiten und ihm dieser Zweck nachweislich mitgeteilt wird. Im heutigen Massengeschäft mit personenbezogenen Daten (Stichwort „Big Data“) ist eine solche „automatisierte (regelbasierte) Einzelfallbehandlung“ nur durch integrierte EDV-Lösungen umsetzbar. Vielleicht ein Einsatzfeld für „smart contracts“, um die Modalitäten der Zurverfügungstellung von personenbezogenen Daten automatisch auszuverhandeln und nachweisbar abzubilden? Oder für jedes personenbezogene Datum wird eine Blockchain angelegt, um dessen „track record“ unveränderbar zu speichern? Der Wirtschaftskreislauf mit dem „Öl des 21. Jahrhunderts“ erfordert anscheinend eine umfangreiche Schutzausrüstung der Beteiligten in Form umfangreicher „Datenprüfungen“ und gegenseitiger „Sicherheitserklärungen“.

Fall 13:
Die Website als Flickenteppich

Praktischer Fall: Die Huber AG hat einen Online-Auftritt. Jeder Browser eines Internet-Nutzers, der die Website der Huber AG aufruft, wird durch den Code der Website zunächst dazu veranlasst, einen Zeichensatz (Font) – Teil der „corporate identity" der Huber AG – von Google-Servern nachzuladen. Weiter wird der Browser dazu veranlasst, bestimmte Java-Funktionsbibliotheken von Drittservern nachzuladen. Diese „Drittdatenquellen", welche der Browser abfragen muss, um die Website der Huber AG überhaupt darstellen zu können, erhalten vom Browser verschiedene Informationen, insbesondere die IP-Adresse des Rechners, auf dem der Browser läuft. Die Dritten haben ihr Einverständnis gegeben, dass ihre Seiten als „Drittdatenquellen" fungieren können, betreiben aber umfangreiches Tracking (Aufbau von Nutzerprofilen) mithilfe der Browser-Daten. Die Huber AG macht sich dazu keine Gedanken.

Niemand muss im Zeitalter des Internets das Rad immer wieder neu erfinden; was verfügbar ist und als gut angesehen wird, das wird als Informationsquelle genutzt. Das betrifft etwa Bilddaten, Zeichensätze, Funktionsbibliotheken mit Code-Fragmenten, Kartendaten, Multimediainhalte, Tracking-Technologien, iFrames und sonstige Daten, die ein Website-Betreiber gerne vorgefertigt einbindet, um Ressourcen zu sparen. Der Benutzer selbst bemerkt gar nicht, dass sein Browser im Hintergrund die Seite mithilfe dieser Ressourcen „zusammenbaut". Da muss es noch gar nicht um urheberrechtliche Fragen, die Gefahr von Schadsoftware, die Zulässigkeit von Werbe-Tracking oder aktiven Elemente von sozialen Medien (Stichwort „Like"-Button) gehen. Zunächst einmal muss die Seite als solche „funktionieren".

Es ist offensichtlich, dass die „Drittdatenquelle" keine Pflichthinweise an den Betroffenen (Website-Besucher) erteilt, dass und welche personenbezogenen Daten sie zu welchen Zwecken verarbeitet. Der Website-Besucher soll ja den Einsatz der „Drittdatenquelle" gar nicht merken; entsprechend wird auch die Zieladresse in der Adresszeile des Browsers nicht angezeigt. In den wenigsten Fällen wird in der Datenschutzerklärung auf den Einsatz von Drittdatenquellen hingewiesen – am ehesten noch auf Google-Maps-Kartenausschnitten. Im oben beschriebenen Fall der Google-Fonts und Funktionsbibliotheken gilt es darüber hinaus zu beachten, dass zu dem Zeitpunkt, zu dem die Datenschutzerklärung für den Betroffenen erstmals überhaupt angezeigt werden kann, die Datenerhebung durch die „Drittdatenquelle" bereits abgeschlossen ist.

Man kann sich in diesen Fällen mit der Antwort des Bayerischen Landesamts für Datenschutzaufsicht in dessen FAQ-Sektion auf die Frage *„Dürfen externe Schriftarten z. B. Google Fonts auf der Website eingebunden werden?“* helfen: *„Ja. Wichtig ist, dass in der Datenschutzerklärung auf der Website darüber informiert wird.“* Auf die entsprechende Frage zur Einbindung von Google Maps lautet die Antwort: *„Ja. Wichtig ist, dass in der Datenschutzerklärung auf der Website darüber informiert wird. Außerdem sollten die Inhalte von Google Maps erst dann geladen werden, wenn der Nutzer aktiv den Kartendienst in Anspruch nimmt, z. B. durch einen extra Klick.“* Das ist pragmatisch, kurz und gut. Es wäre aber noch schöner, wenn sich dieses – für den gesunden Menschenverstand möglicherweise sehr überzeugende – Ergebnis auch aus der DSGVO ableiten ließe. Aber dann ergeben sich leider eine Menge Probleme, die die bayerische Datenschutzaufsicht nicht aufwirft und dementsprechend auch nicht lösen muss. Der Haken ist natürlich, dass die Datenschutzaufsichtsbehörden den Gesetzestext nicht verändern können. Und ob die Antwort des Europäischen Gerichtshofes, wenn er mit dieser Fallgestaltung konfrontiert würde, ebenso simpel ausfallen würde, darf bezweifelt werden.

Der Unterschied zu Fall 12 oben liegt darin, dass hier keine Daten von der Huber AG an die „Drittdatenquelle“ (bzw. den dahinterstehenden Anbieter) direkt übermittelt werden. Vielmehr weist der Code der Webseite der Huber AG den Browser des Webseiten-Besuchers an, mit einem Dritten Kontakt aufzunehmen, der dann gegebenenfalls (neben der IP-Adresse) verschiedene personenbezogene Daten (Browser-Fingerprint etc.) erhebt und dabei gegen Datenschutzrecht verstößt. Diese Konstellation geht über einen (externen) Link, den der Besucher selbst (aktiv) anklickt, hinaus, und erinnert an die Technik der „frames“ (eingebettete Seitenteile aus Drittquellen). Der Jurist denkt dabei an die Konstruktion der „mittelbaren Täterschaft“ unter Einsatz eines „Werkzeugs“, in diesem Fall des ahnungslosen Webseiten-Besuchers, der nur eine Webseite aufrufen wollte und der (bzw. dessen Browser) sodann unwissentlich Informationen an Dritte preisgibt. Datenschutzrechtlich wäre jedoch eher die Frage zu stellen, ob die Huber AG und die „Drittdatenquelle“ – ähnlich wie in den Facebook-Fanpage- und Like-Button-Fällen des EuGH – gemeinsam für Datenschutzverstöße der „Drittdatenquelle“ verantwortlich sind. Im Unterschied zu den EuGH-Fällen profitiert die Huber AG aber nicht an den durch die „Drittdatenquelle“ erhobenen personenbezogenen Daten der Webseiten-Besucher, sondern an den (ihrerseits nicht personenbezogenen) Daten, die von der „Drittdatenquelle“ an den Webseiten-Besucher ausgeliefert werden – also an den zugeladenen Ressourcen. Möglicherweise sind aber die „vermittelten“ personenbezogenen Daten der Webseiten-Besucher die „Währung“, mit der sich die „Drittdatenquelle“ bezahlen lässt, um überhaupt Webseiten-Ressourcen zum Hinzuladen anzubieten.

Auf dieser Basis stellen sich datenschutzrechtlich eine Reihe von Fragen. Ein Hinweis in der Datenschutzerklärung auf die Ressource ist gut und schön, aber müsste der Hinweis nicht erscheinen, bevor auf die Ressource zugegriffen wird? Und auf welcher datenschutzrechtlichen Legitimationsgrundlage erhebt die „Drittdatenquelle" die Daten vom Webseiten-Besucher? Oft sitzt die „Drittdatenquelle" in einem Drittland und es muss eine gesonderte Grundlage für die Drittlandsübermittlung vorliegen – muss nun der Webseiten-Betreiber eine Einwilligung „für den Dritten" einholen, weil schon Daten in das Drittland übermittelt werden müssten, bevor die „Drittdatenquelle" überhaupt selbst eine Einwilligung einholen könnte?

Wenn man solche Ressourcen wie Zeichensatz und Kartenmaterial in der Mitte des Spektrum verortet, dann wäre am einen Ende des Spektrums ein gewöhnlicher Link und am anderen Ende der Facebook-Like-Button zu verorten. Bei letzterem handelt es sich um ein Stück Code von Facebook, das vom Webseiten-Betreiber integriert wird und welches schon beim Aufruf der Webseite „allerhand" Daten an Facebook überträgt, mit denen Facebook dann „allerhand" macht bzw. machen kann. Dies gilt sowohl für den Fall, dass der Webseiten-Besucher selbst Mitglied des sozialen Netzwerks ist, als auch für den Fall, dass der Webseiten-Besucher mit dem sozialen Netzwerk bislang nie etwas zu tun hatte. Die zugrundeliegende Mechanik wurde im Like-Button-Urteil des Europäischen Gerichtshofs vom Juli 2019 („Fashion ID"-Entscheidung) abstrakt so skizziert, dass es ein Webseiten-Betreiber (dort „Fashion ID") einem Dienstebetreiber (dort Facebook) ermöglicht, personenbezogene Daten von den Nutzern der Webseite zu erlangen. Der einfachste Fall des „Zuführens" von personenbezogenen Daten an einen Dritten (verbunden mit der Möglichkeit, auf dieser Basis weitere Daten „abzusaugen") ist die Übermittlung von dessen IP-Adresse. Dies ist aber auch bei jedem normalem Link (oder Frame) der Fall, auf den der Webseiten-Besucher klickt und der zum Laden einer anderen Webseite führt (was vielleicht nicht einmal richtig deutlich für den Nutzer ist, wenn der „Sie verlassen jetzt diese Internet-Seite"-Hinweis fehlt). Natürlich wird der Webseiten-Besucher nach dem Anklicken des Links im Regelfall wissen, dass er sich nun auf einer „anderen Seite" befindet, aber möglicherweise ist ihm das in dem Moment, in dem er den Link anklickt, noch nicht bewusst. Ist der Unterschied zwischen einem (vielleicht nicht als solchem erkennbaren) externen Link, einer (für den Webseiten-Besucher unsichtbaren) externen Ressource und einem (unsichtbaren) „Plug-in" so groß, dass nur ein Plug-in zu einer gemeinsamen Verantwortlichkeit führt, während eine externe Ressource nur „aufklärungspflichtig" ist und ein Link zu einer anderen Webseite unbeachtlich ist?

Dies beschwört eine alte Diskussion über die – umstrittene – Prüfpflicht des „Linksetzers" herauf, die hier dazu führen würde, dass der „Linksetzer" (d. h. der Webseiten-Betreiber) die Datenschutzkonformität der verlinkten Webseite (ständig) prüfen muss, weil er es dessen

Betreiber schließlich auch „ermöglicht, personenbezogene Daten zu erlangen“. Datenschutzrechtlich würde dies noch dazu bedeuten, dass der „Linksetzer“ vollumfänglich und im Vorhinein über die datenschutzrechtlichen Verhältnisse der Zielseite aufklären müsste, denn die Einwilligung des Betroffenen, dass die Zielseite nach dem Klick auf den Link automatisch Daten (zumindest die IP-Adresse) des Betroffenen erhebt, muss – wenn eine solche Einwilligung notwendig ist – wohlinformiert sein. In den FAQ zu Cookies und Tracking des Landesdatenschutzbeauftragten von Baden-Württemberg findet sich der vielsagende, natürlich nicht mit Blick auf Hyperlinks geschriebene Satz:

„Eine ausdrückliche, informierte, freiwillige, aktive und vorherige Einwilligung der Nutzer ist insbesondere erforderlich, wenn Dritten die Möglichkeit gegeben wird, Nutzungsverhalten zu analysieren [...]. Einwilligungs-Banner müssen eingesetzt werden, wenn tatsächlich eine Einwilligung des Nutzers nötig ist, also insbesondere [...] Dritten die Möglichkeit eröffnet wird, Daten zu erheben.“

Wen das Argument der datenschutzrechtlichen „Gefährlichkeit“ von Links nicht überzeugt, der mag sich vor Augen halten, dass Links häufig zusätzliche Informationen über die Verarbeitungssituation „verraten“, die dann mit der – obligatorisch an den Server des „Link-Ziels“ übergebenen – IP-Adresse des Benutzers verknüpft werden. So kann etwa ein Link (vereinfacht gesagt) den Bestandteil „source = twitter“ als Teil der aufgerufenen URL beinhalten, der dem Betreiber des Ziel-Servers die (personenbezogene) Information verschafft, dass der (durch seine IP-Adresse identifizierbare) Benutzer sich entweder auf der Twitter-Plattform aufgehalten hat (und dort den Link angeklickt hat) – diese Information erhofft sich natürlich der Betreiber des Ziel-Servers – oder ihm der Link (zumindest) von einem Twitter-Nutzer weitergeleitet wurde.

Man sieht, dass, wenn man hier einen „rigorosen Kurs fährt“, bei vielen Webseiten erheblich (nachgedacht und) nachgebessert werden muss, eventuell mithilfe von Informationen, die der Webseiten-Betreiber gar nicht hat und sich auf gar nicht beschaffen kann: Er kann nicht ohne Weiteres (s. aber oben Fall 12 zu möglichen „due diligence“-Pflichten in der Datenkette) herausfinden, was der Dritte mit den Daten machen wird, und kann deshalb weder ordnungsgemäße Pflichtinformationen noch später eine vollständige Auskunft erteilen. Dazu muss man gar nicht erst den „Extremfall“ des Facebook-Like-Buttons zugrunde legen.

Fall 14:
Wie tief schaut die DSGVO?, oder:
Alles eine Frage der Granularität

Praktischer Fall: Die Huber AG bewahrt Personalakten bis zehn Jahre nach dem Ausscheiden eines Mitarbeiters auf. Diese Angabe findet sich auch im Verarbeitungsverzeichnis sowie in den Pflichthinweisen gegenüber den Beschäftigten, die diesen zu Beginn des Anstellungsverhältnisses übergeben werden. Begründet wird dies damit, dass z. B. die in der Personalakte befindlichen Lohnabrechnungen entsprechenden steuerlichen Aufbewahrungsfristen unterliegen.

Das sehr generelle Thema „Granularität" zieht sich quer durch die DSGVO, wie auch Fall 11 bereits gezeigt hat. Am Beispiel der Personalakte zeigt sich, dass hierunter eben „eine (einheitliche) Personalakte" verstanden werden kann, die als Ganzes von der Personalabteilung verwaltet und als Ganzes irgendwann vernichtet wird. Doch schon das Steuerrecht („steuerlich relevante Daten") und das Arbeitsrecht (Thema Abmahnungen) zeigen, dass die Personalakte aus verschiedenen Bestandteilen besteht. Für jeden Bestandteil lassen sich daher unterschiedliche Zwecke und daraus folgend Löschfristen identifizieren.

- Granularität der Informationen

Bewerbungen etwa finden sich oft auch nach der Einstellung noch in der Personalakte. Müssen diese, wie bei abgelehnten Bewerbern, spätestens sechs Monate nach der Einstellungsentscheidung gelöscht werden? Oder darf die theoretische Möglichkeit, das Arbeitsverhältnis wegen arglistiger Täuschung, etwa wegen erfundener Zeugnisse, anzufechten, als Rechtfertigung für eine Zehnjahresfrist herangezogen werden (§ 124 Abs. 3 BGB)? Lohnabrechnungen hingegen unterliegen steuerlichen Aufbewahrungsfristen, die sich im Falle einer „spät begonnenen" Betriebsprüfung sogar situationsabhängig („Ablaufhemmung") verlängern können. Abmahnungen müssen aus arbeitsrechtlichen Gründen sechs Monate nach ihrem Ausspruch „vergessen" werden, weil sie keine Wirkungen mehr entfalten – oder sind sie für eine spätere Leistungsbeurteilung oder ein Zeugnis noch „erforderlich"? Ist der Anstellungsvertrag auch nach dem Ausscheiden des Mitarbeiters weiter aufzubewahren? Wie steht es mit Leistungsbeurteilungen durch Vorgesetzte, Zwischenzeugnisse, Arbeitsunfähigkeitsbescheinigungen, in Schließanlagen gespeicherte Öffnungsvorgänge mit personalisierten Schlüsseln? Worüber muss der Arbeitgeber auch später noch Auskunft geben können, weshalb kann er wie lange noch in Anspruch genommen werden?

➢ Was man hat, das gibt man ungern wieder her

Bei all dem ist generell zu berücksichtigen, dass Verjährungsfristen nicht zum datenschutzrechtlichen „Behalt auf Verdacht" berechtigen. Einerseits kann von einer Löschung nur abgesehen werden (Art. 17 Abs. 3 lit. e DSGVO), wenn die Geltendmachung von Ansprüchen unmittelbar bevorsteht bzw. konkrete Anzeichen für ein Vorgehen vorliegen. Dies hat beispielsweise die österreichische Datenschutzbehörde in einem Bescheid vom Mai 2018 – unmittelbar nach Inkrafttreten der DSGVO – hinsichtlich der Aufbewahrung von Stamm- und Verkehrsdaten eines Telekommunikationsunternehmens festgehalten: Eine Verjährungsfrist normiere keine „konkrete Verpflichtung zur Aufbewahrung von Daten". Dabei wurde auch ergänzt, dass gesetzliche Aufbewahrungspflichten nicht „mit der Berufung auf interne Prozesse bzw. den Postlauf" ausgedehnt werden dürften. Wenn man sich vor Augen hält, wie oft in Löschkonzepten – gelinde gesagt – „Sicherheitspuffer" eingebaut werden, müsste das eigentlich für Beunruhigung sorgen. Und auch das Bayerische Landesamt für Datenschutzaufsicht führt in seinem Tätigkeitsbericht 2017/2018 – mutmaßlich zum Entsetzen aller Ersteller von (auf pauschalen Fristen basierenden) Löschkonzepten in Großunternehmen – aus:

„Eine Ausnahme von der Verpflichtung zur Löschung kann sich zudem aus Art. 17 Abs. 3 Buchstabe e DS-GVO ergeben, da die objektive Verjährungsfrist für Schadensersatzansprüche wegen Körper- oder Gesundheitsverletzungen gemäß § 199 Abs. 2 BGB dreißig Jahre nach Vornahme des potentiell schadensträchtigen Verhaltens beträgt. Hier ist eine Abwägung unter Berücksichtigung der Interessen des Betroffenen und der Wahrscheinlichkeit der Geltendmachung von Ansprüchen („erforderlich") vorzunehmen. Eine Aufbewahrung aller Patientendaten für die Dauer von 30 Jahren wegen drohender Schadensersatzansprüche wäre nicht datenschutzkonform. Erforderlich ist hier eine individuelle Risikobewertung."

Und andererseits ist das Vorliegen der Voraussetzungen dieser Ausnahme von der Löschpflicht nicht genug, um die Daten tatsächlich behalten zu dürfen. Denn wie immer bedarf es einer Legitimationsgrundlage für die Verarbeitung, die Art. 17 Abs. 3 DSGVO (wohl) nicht darstellt. Der deutsche Gesetzgeber hat dafür eigens – als spezielle Form der Interessenabwägung – eine Legitimationsgrundlage in § 24 Abs. 1 Nr. 2 BDSG geschaffen, wobei diese Regelung ausdrücklich an einen vorherigen anderweitigen (und entfallenen) Zweck anschließt (*„zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden"*). Wenn das nicht weiterhilft, stehen auch noch Art. 6 Abs. 1 S. 1 lit. f DSGVO sowie – für besondere Kategorien personenbezogener Daten – § 24 Abs. 2 BDSG bzw. Art. 9 Abs. 2 lit. f DSGVO zur Verfügung. Dies bedeutet aber auch, dass nicht „alle" Daten „einfach so" für

Zwecke der Rechtsdurchsetzung oder Rechtsabwehr aufbewahrt werden dürfen, sondern dass eine Abwägung der Interessen im Einzelfall notwendig ist.

Dies zeigt deutlich: Dass der Verantwortliche generell alle Daten gerne lange aufbewahren würde, weil er diese „irgendwann" vielleicht noch für eine möglicherweise zu einem späteren Zeitpunkt (während der Verjährungsfristen) begonnene Auseinandersetzung benötigt, kann als solches kein Argument für eine Aufbewahrung bis zum Ende der Verjährungsfrist sein. Dies gilt insbesondere für „längere" Verjährungsfristen, während bei kurzen Verjährungsfristen (etwa nach dem Allgemeinen Gleichbehandlungsgesetz für Klagen abgewiesener Bewerber, für die eine Sechs-Monats-Frist einschlägig ist) auch die Datenschutzbehörden einfach mal „die Augen zudrücken" und eine Speicherung für die Dauer der Verjährungsfrist akzeptieren (so beispielsweise auch das Bayerische Landesamt für Datenschutzaufsicht in seiner FAQ-Sektion auf die Frage *„Wie lange darf ich die Daten von Bewerbern speichern?"*). Manchmal hilft zwar (scheinbar) eine Aufbewahrungsfrist aus dem Dilemma, die ähnlich lang wie die Verjährungsfrist ist. So bestimmt beispielsweise § 28 Abs. 3 der RöntgenVO, dass Aufzeichnungen über Röntgenbehandlungen (also über Behandlungen – nicht Untersuchungen – mit Röntgenstrahlen) 30 Jahre nach der letzten Behandlung aufzubewahren sind, während die Röntgenbilder selbst und Aufzeichnungen über Röntgenuntersuchungen 10 Jahre aufzubewahren sind. Ähnlich ist es mit den inhaltlich weitreichenden steuerlichen und handelsrechtlichen Aufbewahrungspflichten.

Ob die nur zu diesem sehr limitierten Zweck der gesetzlichen Aufbewahrungspflicht noch aufbewahrten Daten dann später (auch oder nur noch) für die Rechtsdurchsetzung oder Rechtsabwehr „zweckentfremdet" werden dürfen, wenn sich diese Notwendigkeit erst während der Aufbewahrungsfrist ergeben hat, ist eine andere Frage. § 24 Abs. 1 Nr. 2 BDSG deutet eher in die Richtung, dass sich zu dem Zeitpunkt, zu dem der ursprüngliche Erhebungszweck entfallen oder erreicht ist, eine Aufbewahrung direkt anschließen kann, wenn dies für eine zu diesem Zeitpunkt konkret absehbare Streitigkeit erforderlich ist. Ist zu diesem Zeitpunkt aber gar keine Streitigkeit absehbar und hat über die Aufbewahrungspflicht (Art. 6 Abs. 1 S. 1 lit. c DSGVO) bereits eine erste Zweckänderung stattgefunden, so würde sich eine Verwendung zu Zwecken der Rechtsdurchsetzung oder Rechtsabwehr, die erst „mitten" im Aufbewahrungszeitraum entsteht, nicht mehr an den ursprünglichen Erhebungszweck anschließen, sondern „nur noch" an einen bereits sekundären Zweck. Es wäre dann schon die zweite Zweckänderung. Mit anderen Worten: Der Verantwortliche würde vom „Zufall", dass die Daten einer gesetzlichen Aufbewahrungsfrist unterlagen (und nur deshalb liegen sie ihm zum Zeitpunkt einer konkreten Auseinandersetzung noch vor), im Hinblick auf die

Rechtsdurchsetzung bzw. Rechtsabwehr profitieren dürfen. Er wird gegenüber einem Verantwortlichen, der die Daten bereits nach dem Ende des Erhebungszwecks unmittelbar löschen musste, besser gestellt. Vielleicht ist diese Lesart von § 24 BDSG aber auch zu eng.

- Kategoriebildung

In der Praxis wird man sich in dieser Gemengelage mit „gerasterten" Lösungen behelfen müssen, d. h. die Daten werden typisiert im Rahmen eines Löschkonzepts in Kategorien eingeteilt, die im Wesentlichen anhand von Aufbewahrungs- und Verjährungsfristen gebildet werden. Dass dabei erfahrungsgemäß in der Mehrzahl der Fälle, die mit der Begründung einer noch laufenden Verjährungsfrist weiter aufbewahrt werden, gar keine konkrete Rechtsdurchsetzung oder Rechtsabwehr notwendig wird (oder pauschal die längste – aber nur für einen Teil der Daten einschlägige – Aufbewahrungspflicht angenommen wird), fällt dabei leicht unter den Tisch und wird daher auch von den Datenschutzbehörden kritisiert.

Unabhängig vom exorbitanten Aufwand von Einzelfallprüfungen und Einzel-Interessenabwägungen begründet aber eine Löschung vor dem Ende der Verjährungsfristen die erhebliche Gefahr für den Verantwortlichen, sich im Falle einer späteren, nicht konkret vorhersehbaren Inanspruchnahme nicht verteidigen zu können und sogar im Falle eigentlich haltloser Ansprüche zu unterliegen. Man kann mit diesem (pauschalen) Argument das Interesse des Verantwortlichen an einer Fortspeicherung von Daten, die für noch unverjährte Ansprüche erforderlich sind, durchaus auch (pauschal) hoch gewichten – mit unvorhersehbarem Ausgang bei einem Streit über die Legitimität dieser Fortspeicherung. Übersehen wird in diesem Zusammenhang zudem, dass eine „wirklich effektive" Einzelfallbetrachtung, ob nun eine Streitigkeit konkret droht oder nicht, neben exorbitantem Aufwand auch ein Vielfaches der Daten, um die es eigentlich geht, erfordern kann. Man würde also sprichwörtlich den Teufel mit dem Beelzebub austreiben und die Erhebung von weiteren Daten herausfordern.

Daher werden in der juristischen Literatur durchaus auch sehr „grobkörnige" Lösungen vertreten, etwa die Einordnung sämtlicher E-Mails eines (beliebig großen) Unternehmens in lediglich drei Aufbewahrungskategorien. Dabei wird in der jeweiligen Kategorie die „pauschale Anwendung der längsten für den Verantwortlichen geltenden" Verjährungs- oder Aufbewahrungsfrist als angemessen betrachtet. Speziell für steuerliche Aufbewahrungspflichten wird dabei darauf hingewiesen, dass ein finanzielles Risiko in Gestalt der Schätzung von Besteuerungsgrundlagen (§ 162 Abgabenordnung) droht, sofern relevante aufzubewahrende Informationen zu früh gelöscht werden. Letztlich wird also eine – in der DSGVO genaugenommen nicht vorgesehene – Abwägung zwischen dem in einer grobkörnigen Kategorisie-

rung liegenden Risiko und dem bei einer feinkörnigen Kategorisierung notwendigen Aufwand vorgenommen. Dabei handelt es sich tatsächlich um eine Risikoabwägung und nicht „nur" um eine (entsprechend des ermittelten Risikos identifizierte) technische und organisatorische Maßnahme: Die Fortspeicherung auch nur eines einzigen Datums ohne entsprechende Legitimationsgrundlage ist „eigentlich" ein Datenschutzverstoß, der nicht durch Kostenerwägungen ungeschehen gemacht werden kann. Dies gilt auch für (vermeintliche) „Niedrigrisikodaten", also Daten, hinsichtlich derer ein Verantwortlicher davon ausgeht, dass mit ihnen nicht viel „Schindluder" getrieben werden kann. Das in der juristischen Literatur in diesem Zusammenhang vorgebrachte Argument, ein E-Mail-Archiv eines Unternehmens erlaube naturgemäß kein Profiling der Betroffenen oder Verarbeitungen zu Zwecken der Datenanalyse, ist mit großer Vorsicht zu genießen.

Und nur nebenbei stellt sich im Zusammenhang mit der Kategorisierung bei Löschkonzepten nicht nur das Problem der Bildung der Kategorien, sondern auch und gerade des Vorgangs der Zuordnung zu den einzelnen Kategorien. Auch wenn keine datenschutzrechtliche Einzelfallprüfung durch ein Heer von (Unternehmens-)Juristen stattfindet, schafft selbst ein manueller „Sortieraufwand" anhand von entsprechenden Prozessvorgaben an die Beschäftigten im täglichen Arbeiten einen nicht unerheblichen Mehraufwand und setzt entsprechende „Archivierungsdisziplin" voraus. Fällt dabei zu viel durch das – wie auch immer definierte – Raster und landet in der falschen Kategorie, kann nur noch schlecht mit einem unvermeidbaren „Ausreißerfehler" argumentiert werden: Dann war der Prozess – sprich: die organisatorischen Maßnahmen – nicht strikt genug vorgegeben.

- Je größer die Lupe desto schwieriger die Compliance

Man kann die eigentlich notwendige „Atomisierung" im Rahmen der individuellen Einzelfallbetrachtung, zu der im Streitfall auch Gerichte in Bezug auf das konkret streitgegenständliche Detail neigen könnten (der Rechtsstreit als Sachverhalts-„Lupe"), nicht nur in Bezug auf die (in ihrem Umfang nicht definierten) „Datenkategorien" im Kontext eines Löschkonzepts betreiben. Fall 11 zeigt das Gleiche in Bezug auf die Verarbeitungstätigkeiten. Beispielsweise führt die Ausfüllhilfe des bayerischen Landesamts für Datenschutzaufsicht („Erste Hilfe zur DSGVO") bei der Verarbeitungstätigkeit „Personalverwaltung" zur Rubrik „Empfänger, gegenüber denen die personenbezogenen Daten offengelegt werden" lediglich die Empfänger Sozialversicherungsträger und die Finanzbehörden auf. Müssen aber nicht auch die Banken genannt werden, über die Löhne und Gehälter stets ausbezahlt werden und denen die Daten der Empfängerkonten weitergegeben werden? Je „atomarer" man also Prozesse, Datenkategorien, Betroffene, Löschanforderungen etc. zerlegt, desto unwahrscheinlicher wird es, die DSGVO vollständig erfüllen und damit den Sanktionen sicher entgehen zu können. Denn

dem uferlos formulierten Anspruch der DSGVO kann nur und erst dann vollständig entsprochen werden, wenn jedes „Atom“ aus DSGVO-Perspektive vollständig identifiziert, bestimmt, nachweisbar rechtmäßig behandelt und dies jeweils nachverfolgbar wäre. In der Praxis gerät jedes System (weit) vorher an seine Grenzen. Nach mündlichen Aussagen von Mitarbeitern der Datenschutzbehörden wird daher (nur) eine „mittlere Granularität“ gefordert – was immer das bedeutet und woraus auch immer sich das ableiten mag.

➢ Ein Betroffener kommt selten allein

Dabei sei zum Abschluss auch noch auf das weite Feld der „Drittbetroffenen“ hingewiesen. Schreibt ein Angestellter in Elternzeit morgens an die Personalabteilung, er könne nicht kommen, weil er sein Kind mit Verdacht auf Lungenentzündung in ein Krankenhaus bringen musste, so enthält diese E-Mail personenbezogene Daten des (identifizierbaren) Kindes. Mit den Regelungen, mit denen die Verarbeitung personenbezogener Daten – auch Gesundheitsdaten – von Beschäftigten rechtfertigt werden kann (§ 26 BDSG), kann die Ablage dieser E-Mail „eigentlich“ nicht rechtfertigt werden. Und auch die üblichen „E-Mail-Weiterleitungsketten“ enthalten häufig „weiter unten“ mannigfaltige personenbezogene Daten Dritter, die oft nicht einmal wissen, dass ihre E-Mail weitergeleitet wurde und wer diese E-Mail nun alles ansieht, speichert oder weitersendet. Werden bei der Einstellung eines Mitarbeiters die Daten eines Angehörigen erfasst (Notfallkontakt, Angehörige der Familienversicherung), stellt auch dies eine „Drittdatenerhebung“ dar, die ebenfalls in der Regel die Pflichtinformationen des Art. 14 DSGVO notwendig macht (s. dazu aber auch unten Fall 22). Bemerkenswert sind in diesem Zusammenhang auch die Ausführungen der Berliner Beauftragten für Datenschutz in ihrem Jahresbericht 2018 zum Thema „stilles Factoring“:

„Soweit das die Forderung aufkaufende Unternehmen keine Schuldnerdaten erhält oder die Schuldnerin eine juristische Person ist, ist stilles Factoring weiter unproblematisch möglich. Werden aber personenbezogene Daten an neue Gläubiger übermittelt, sind die Transparenzpflichten von Forderungsverkäufern (Art. 13 DSGVO) und Forderungskäufern (Art. 14 DSGVO) zu beachten. Forderungsverkäufer werden zumindest bei Vertragsschluss allgemein darüber informieren müssen, dass eine Datenübermittlung im Zusammenhang mit einem Forderungsverkauf ggf. erfolgt (Art. 13 Abs. 1 lit. e DSGVO). Auch Forderungskäufer haben Informationspflichten. Dies ist zwar nicht der Fall, wenn nationales Recht die Erlangung oder Offenlegung durch Rechtsvorschrift regelt, denen die Verantwortlichen unterliegen und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Personen vorsehen (Art. 14 Abs. 5 lit. c DSGVO). Es ist aber nicht anzunehmen, dass die BGB-Normen als solche Rechtsvorschriften anzusehen sind. Insbesondere ist darauf hinzuweisen, dass ein Forderungskäufer nicht das Recht hat, eine Bonitätsprüfung der Schuldnerin

oder des Schuldners durchzuführen, da diese bei Vertragsabschluss nicht damit rechnen mussten, dass Dritte, mit denen sie keinen Vertrag abschließen wollten, Abfragen bei Auskunfteien vornehmen würden, die zu einer Verschlechterung ihres Scoring-Werts führen können. Stilles Factoring sollte nur ohne Übermittlung von Schuldnerdaten erfolgen."

Man kann sogar – aber das soll hier nicht vertieft werden – darüber nachdenken, ob eine Forderungsabtretung, deren Durchführung gegen Datenschutzrecht verstößt, nicht auch zivilrechtlich unwirksam ist (§ 134 BGB). Der Bundesgerichtshof hat dies zwar in einem Urteil vom Februar 2007 für einen Verstoß gegen das damalige Bundesdatenschutzgesetz bei einer Forderungsabtretung zwischen Banken verneint. Das „Totschlagsargument" war dabei, dass datenschutzrechtliche Verbotsnormen den Grundsatz der freien Abtretbarkeit von Forderungen aushebeln und in sein Gegenteil verkehren würde. Man könnte es auch so formulieren: Wir lassen uns vom neumodischen Datenschutzrecht nicht unsere altmodischen BGB-Grundfesten vermiesen. Gewichtiger scheint noch das Argument zu sein, dass durch eine unwirksame Forderungsabtretung nichts gewonnen ist: Die (unterstellt) rechtswidrig übermittelten Schuldnerdaten sind nun einmal beim Forderungserwerber faktisch angekommen. Das Ganze mag dann ein Bußgeld auslösen oder Schadensersatzforderungen oder sogar strafbar sein (§ 42 Abs. 1 BDSG), aber die Unwirksamkeit der Forderungsabtretung hilft nicht dagegen, dass personenbezogene Daten datenschutzwidrig „in der Gegend herumstreunen". Man wird sehen, ob dieses „Fass" unter der Geltung der DSGVO noch einmal neu aufgemacht wird. Ebenso wie bei der Frage der Abmahnbarkeit von DSGVO-Verstößen wird dabei eine große Rolle spielen, ob die Sanktionen der DSGVO abschließend in dieser selbst festgelegt wurden oder ob noch weitere Sanktionsmechanismen aus nationalstaatlichem Recht zusätzlich eingreifen dürfen.

Zum Abschluss noch ein weiteres Beispiel in Sachen Drittbetroffenheit. Im Falle der Übermittlung von Daten für eine Traueranzeige hält – im Gegensatz zur Berliner Beauftragten für Datenschutz – das bayerische Landesamt für Datenschutzaufsicht in seinem Tätigkeitsbericht 2017/2018 ausdrücklich nicht den Empfänger der Daten für verpflichtet im Sinne von Art. 14 DSGVO gegenüber den Drittbetroffenen, sondern geht nach dem „Veranlassungsprinzip" vor:

„Bei der Aufgabe von gedruckten Traueranzeigen oder für Online-Medien muss der Veranlasser der Traueranzeige die übrigen darin genannten Personen (z. B. Angehörige) hierzu informieren, nicht etwa die Zeitung oder der Dienst selbst. Was in einer solchen Anzeige genau steht und welche Trauernde dabei namentlich genannt werden, liegt im Verantwortungsbereich der Person, die eine Traueranzeige selbst oder über einen Bestatter aufgibt.

Wir haben daher festgehalten, dass diese Person (z. B. ein Angehöriger) sich bei den betroffenen Personen vergewissern muss, ob und in welcher Weise sie in der Traueranzeige genannt werden wollen, bevor sie eine Zeitung und gegebenenfalls deren Online-Dienst mit der Veröffentlichung beauftragt.“

Eine dogmatische Begründung, warum hier die Pflicht des Empfängers zur Pflichtinformation der Betroffenen entfällt, fehlt hier – es sei denn, man geht generell davon aus, dass das „Übermittelt-Erhalten“ kein Fall der Erhebung des Art. 14 DSGVO darstellt (s. oben Fall 1). Wer weiß, welche weiteren Probleme unter der „granularen Lupe“ noch sichtbar werden.

Fall 15:
Gibt es eigentlich noch Daten, die nicht personenbezogen sind?

Praktischer Fall: Herr Huber ist Mehrheits-Kommanditaktionär der „Huber Metallverarbeitung GmbH & Co. KGaA", während Inhaber der Gesellschaftsanteile sowie Geschäftsführer der Komplementärin, der „Huber Metallverarbeitung Verwaltungs GmbH", sein Schwager, Herr Meier, ist. Ein Abnehmer der „Huber Metallverarbeitung GmbH & Co. KGaA", die Schulze AG, erhebt eine interne Statistik über ihre Lieferanten und das jährliche Umsatzvolumen mit diesen Lieferanten, in der für die „Huber Metallverarbeitung GmbH & Co. KGaA" und das Jahr 2018 die Zahl „2,4 Mio. EUR" angegeben ist.

Die DSGVO beginnt mit einem Paukenschlag in Form eines Zirkelschlusses: Personenbezogene Daten sind Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, wobei als identifizierbar eine natürliche Person angesehen wird, die direkt oder indirekt identifiziert werden kann (Art. 4 Nr. 1 DSGVO). Hier wird also nicht einmal nur ein abstrakter Begriff durch einen anderen abstrakten Begriff ersetzt – wie es Juristen so gerne mögen –, sondern durch denselben. Identifizierbarkeit ist die Möglichkeit einer Verknüpfung zwischen natürlicher Person und einem „Identifier" (wie einer Versicherungsnummer oder einer IP-Adresse), sodass zwischen beiden Identität hergestellt werden kann. Man stelle sich also einen Datenverarbeiter oder einen „Angreifer" vor, der diese Verknüpfung herstellen möchte, und frage, welche Fähigkeiten (Mittel), welches Wissen (Vergleichsdatenbestand) und welche Rationalität (Vorgehensweise) dieser Person „nach allgemeinem Ermessen wahrscheinlich" (Erwägungsgrund 26 zur DSGVO) unterstellt werden kann. Irgendwann ist diese Person dann „identifizierbar". Wieder einmal türmen sich die „Begriffspyramiden", weshalb es sogar Vorschläge gibt, den Personenbezug im Datenschutzrecht insgesamt als veraltet und nicht praktikabel abzuschaffen.

➢ Wann sind Daten auf Personen beziehbar?

Zur Identifizierbarkeit der Person des Betroffenen kommt der Personenbezug der Daten selbst: Sämtliche Informationen, die sich auf den Betroffenen „beziehen", sind „personenbezogene" Daten. Was bezieht sich nicht auf Personen? Vielleicht Dinosaurierfunde aus dem Mesozoikum, als es noch keine Menschen gab? Oder kann nicht auch jeder Dinosaurierknochen einem Paläontologen zugeordnet werden, der diesen ausgegraben und beschriftet hat? „Bezieht" sich das Foto eines Pflanzenbeets auf den Gärtner, der das Beet angelegt hat, oder

auf den Fotografen, der den Bildausschnitt gewählt hat? „Bezieht" sich Kommunikation zwischen Maschinen auf den Erfinder der Maschine, den Programmierer der Software, den Bediener der Maschine (Autofahrer)? „Bezieht" sich der Wert eines Grundstücks auf den Eigentümer, der die aus dem Wert abgeleitete Grundsteuer zu zahlen hat? „Bezieht" sich die Anmerkung eines Prüfers am Rande einer Klausur auf den Prüfling? „Bezieht" sich die handschriftliche Anmerkung „Maier: Er will keinen höheren Preis zahlen" in einem anwaltlichen Protokoll einer Verhandlung, das gescannt und Teil der elektronischen Handakte des Anwalts wird, auf Herrn Maier? „Bezieht" sich die Information „Genehmigt durch die Buchhaltung" auf Frau Huber, die die einzige Mitarbeiterin der Buchhaltungsabteilung der Firma Müller ist? „Bezieht" sich der gesamte Sonderprüfungsbericht eines Wirtschaftsprüfers, in dem mögliche Verfehlungen einer natürlichen Person untersucht werden, auf diese Person? Das Wort „Bezug" verfügt über eine sehr große begriffliche Unschärfe – Stichwort „Graukeil". Man mag sich in allen diesen Beispielen vorstellen, wie es datenschutzrechtlich „weitergeht": Pflichthinweise bei Erhebung, Auskunftsrecht, technische und organisatorische Maßnahmen etc. etc.

- Daten juristischer Personen

In diesem Zusammenhang ist auch noch auf eine andere, wenig beachtete Diskussion hinzuweisen, nämlich, inwieweit auch Daten, die nicht auf natürliche Personen, aber auf juristische Personen (insbesondere Unternehmen) als solche bezogen sind, „Datenschutz" genießen. Das „alte" deutsche Datenschutzrecht wurde in einigen Gerichtsentscheidungen wie selbstverständlich analog auf Unternehmen angewandt und diese Analogie mit den auch für Unternehmen geltenden Grundrechten begründet. Es war nur immer unklar, ob dies ausschließlich gegenüber staatlichen Datenerhebungen gelten soll oder auch – über die im Datenschutzrecht besonders weitgehende „Drittwirkung der Grundrechte" – im normalen privatwirtschaftlichen Geschäftsverkehr.

Nach Erwägungsgrund 14 gilt die DSGVO *„nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person"*. Dies kann allerdings nach einhelliger Meinung in der juristischen Literatur nur gelten, soweit diese Daten ausschließlich im Kontext der juristischen Person verarbeitet werden. Erfolgt hingegen die Verarbeitung erkennbar mit Inhalts-, Zweck- oder Ergebnisbezug zu der hinter der juristischen Person stehenden natürlichen Person, sind die Vorgaben der DSGVO auf diese Verarbeitung anzuwenden.

Verschiedene Staaten in der EU haben sowohl den Geltungsbereich der Vorläuferregelung, der EU-Datenschutzrichtlinie, als auch die DSGVO selbst auf juristische Personen erweitert. Europarechtlich spricht nichts dagegen, den Wirkungskreis der DSGVO regional größer zu ziehen, auch wenn dadurch ein inhomogener Datenschutz in der EU etabliert wird.

- Mittelbare Personenbeziehbarkeit auf einen Inhaber

Wie oben angedeutet, können aber auch unter der DSGVO selbst Daten, die sich vordergründig „nur" auf eine juristische Person beziehen – im Beispielsfall auf die „Huber Metallverarbeitung GmbH & Co. KGaA" –, einen Bezug zu der/den „hinter" dem Unternehmen stehende(n) natürliche(n) Person(en) herstellen. Der EuGH sagt dazu, dass der Name einer juristischen Person eine oder mehrere natürliche Personen „bestimmen" kann. Ebenso kommt es vor, dass einer natürlichen Person eine juristische Person unmittelbar oder mittelbar „gehört" und deshalb Aussagen über die juristische Person auch eine signifikante Aussage über die natürliche Person darstellen. In diesem Fall gilt die DSGVO auch für unternehmensbezogene Daten mit Personenbezug, d. h. die Umsatzangabe sagt nicht nur etwas über die „Huber Metallverarbeitung GmbH & Co. KGaA" aus, sondern ist auch ein personenbezogenes Datum betreffend Herrn Huber selbst. Da kann man beinahe froh sein, dass Gottlieb Daimler schon vor Langem gestorben ist.

Das soll nun nicht bedeuten, dass sich jedes Datum, dass sich auf eine juristische Person bzw. Gesellschaft oder Institution bezieht, auch auf die natürliche Person „hinter" der juristischen Person – vorausgesetzt es gibt eine solche – bezieht. Sicher wird es keine Aussage über eine „hinter" der Gesellschaft stehende Person ermöglichen, wenn die Gesellschaft einen neuen Schreibtisch für ihren Prokuristen erwirbt. Aber wenn eine Gesellschaft ein Darlehen aufnimmt und dieses notleidend wird, bezieht sich diese Information dann auch auf den Alleingesellschafter der Gesellschaft? Oder kann nur dann eine signifikante Aussage über den Alleingesellschafter getroffen werden, wenn dessen Gesamtvermögen im Wesentlichen aus der Beteiligung an der Gesellschaft besteht? In diesem Fall würde ein Tilgungsausfall, eine Sicherheitenverwertung und Ähnliches den Schluss zulassen, dass es der natürlichen Person „hinter" der Gesellschaft finanziell „nicht gut geht".

Das Problem besteht hier nicht nur in einer „Relevanzschwelle", d. h. dass die unternehmensbezogenen Daten eine relevante Aussage über die natürliche Person ermöglichen müssen, um personenbeziehbar zu sein. Vielmehr können verschiedene unternehmensbezogene Einzeldaten, die aus unterschiedlichen Quellen zusammengetragen und „verkettet" werden, zusammengenommen Aussagen über natürliche Personen ermöglichen, die nur anhand einzelner Einzeldaten nicht möglich wären. Beispielsweise ist für die Frage, ob der Umstand,

dass ein der Gesellschaft eingeräumtes Darlehen notleidend wird, auch auf die natürliche Person „hinter" der Gesellschaft „durchschlägt", die (weitere) Information entscheidend, ob die natürliche Person ihr Vermögen zu einem großen Teil in dieser Gesellschaft hält. Nur wer beides „weiß", kann einen Schluss auf die aktuelle Vermögenssituation der natürlichen Person „hinter" der Gesellschaft ziehen. Da die Frage der Personenbeziehbarkeit von Daten als „on/off"-Kriterium den Anwendungsbereich der DSGVO eröffnet bzw. nicht eröffnet – die DSGVO gilt nur für personenbezogene Daten –, würde die DSGVO noch nicht bei Kenntnis der Einzeldaten einschlägig sein. Vielmehr würde die Information, dass das Darlehen notleidend ist, erst dadurch zu einem personenbezogenen Datum für einen bestimmten Verantwortlichen werden, dass dieser die Relation zwischen Gesamtvermögen und dem in der betreffenden Gesellschaft gebundenen Vermögen kennt. Dabei geht es nicht um die „Identifizierbarkeit" des Betroffenen im Sinne von Art. 4 Nr. 1 DSGVO, von Erwägungsgrund 26 und der Rechtsprechung des Europäischen Gerichtshofs zur dynamischen IP-Adresse, sondern um den Personenbezug an sich (als weiteres Kriterium für das Vorliegen eines personenbezogenen Datums). Die DSGVO wäre daher erst in dem Moment anwendbar, in dem diese (sämtliche) Einzeldaten beim Verantwortlichen vorliegen und damit der Personenbezug (tatsächlich) vorliegt. Dann wäre aber das Risiko, dass ein „Täter" die notwendigen Daten aus verschiedenen Quellen zusammenträgt und verkettet, für den Verarbeiter eines einzelnen, nicht personenbezogenen Datums – etwa des Umstands, dass das der Gesellschaft eingeräumte Darlehen notleidend geworden ist – datenschutzrechtlich irrelevant, weil sein „Teildatum" nicht Gegenstand der DSGVO wäre.

- Mittelbare Personenbeziehbarkeit auf Organe

Das Beispiel des notleidenden Darlehens, das an eine Gesellschaft ausgegeben wurde, kann aber nicht nur Schlüsse auf die wirtschaftliche Situation des hinter der Gesellschaft stehenden „Inhabers" zulassen. Vielmehr kann sich aus gesellschaftsbezogenen Daten auch eine Information über die (mutmaßliche) Verantwortlichkeit natürlicher Personen ergeben. Jemand, der über die Daten über ein schleppendes Zahlungsverhalten einer Gesellschaft gegenüber ihren Gläubigern verfügt, kann daraus folgern, dass sich der Geschäftsführer in einer Insolvenzverschleppungssituation befindet, für die er persönlich haftet (Insolvenzantragspflicht). Auch hierfür wird es notwendig sein, verschiedene Einzeldaten zusammenzutragen und zu bewerten, die diesen Schluss für sich genommen jeweils noch nicht zulassen. Und auch hier würde den einzelnen Daten, soweit sie nur an die Gesellschaft anknüpfen (die Gesellschaft bezahlt ihre Rechnungen seit einiger Zeit nicht pünktlich), noch kein Schutz unter der DSGVO zukommen. Würde man dies anders sehen wollen, könnte wohl aus jedem gesellschaftsbezogenen Datum potenziell – im Rahmen irgendeiner „Story" bzw. eines Szenarios – auch eine Aussagewirkung im Hinblick auf natürliche Personen entnommen

werden. Damit wäre die Beschränkung der DSGVO auf personenbezogene Daten „hinterrücks“ entwertet und der Erwägungsgrund 14 zumindest irreführend.

Wo genau verläuft also hier die „rote Linie“? Es scheint, als habe sich bislang noch niemand vertieft mit dieser Frage beschäftigt, obwohl doch viele unternehmensbezogene Daten kursieren und hinter vielen Gesellschaften Privatpersonen stehen bzw. jede Gesellschaft über Organe verfügt.

- Werturteile

Ein weiteres Problemfeld bei der Beantwortung der Frage, wo „personenbezogene Daten“ eigentlich aufhören bzw. anfangen, stellt sich bei subjektiven oder errechneten Werturteilen eines Verantwortlichen über einen Betroffenen anhand personenbezogener Daten. In einer Verwaltungsstrafe der österreichischen Datenschutzaufsichtsbehörde vom Oktober 2019 über EUR 18 Mio. (s. zu einem anderen Aspekt des Falles auch noch unten Fall 28) wurde unter anderem die statistische Herleitung einer (vermuteten) „Parteiaffinität“ aus den der österreichischen Post vorliegenden Daten über Betroffene thematisiert. Die Parteiaffinität wäre natürlich ein personenbezogenes Datum, wenn sie vom Betroffenen selbst mitgeteilt würde. Aber ist sie auch ein personenbezogenes Datum, wenn man sie schätzt? Wenn dies so wäre, könnte darüber hinaus Art. 9 DSGVO für die zugrundeliegenden „Basisdaten“ einschlägig sein, denn dort heißt es, dass die Verarbeitung personenbezogener Daten, *„aus denen [...] politische Meinungen [...] hervorgehen“*, den zusätzlichen Erfordernissen des Art. 9 DSGVO unterliegen. Kann dies aber auch dann gelten, wenn man mit statistischen Mitteln aus Daten, die mit der politischen Meinung zunächst wenig zu tun haben – wie Adresse, Geburtsdatum etc. –, eine vermutete Parteiaffinität ableitet?

Eine ähnliche Fragestellung behandelt ein Urteil des LG Karlsruhe vom August 2019. Dort hatte eine Auskunftei einen „Basisscore“ über Betroffene gebildet, der aus Sicht des klagenden Betroffenen zu niedrig ausgefallen war, da er stets seine Rechnungen gegenüber seinen Gläubigern pünktlich bezahlt habe. Nach Ansicht des LG Karlsruhe ist der Scorewert ein subjektives Werturteil und kein personenbezogenes Datum. Lediglich unrichtige personenbezogene Daten dürfen in die Ermittlung des Scorewertes nicht einbezogen werden. Das Ergebnis ist nach dieser Entscheidung nicht mehr Gegenstand des Datenschutzrechts. Darüber hinaus stellt das LG Karlsruhe klar, dass selbst die Annahme einer Datenschutzverletzung den vom Kläger begehrten Schadensersatz nur dann rechtfertigen würde, wenn eine konkrete, tatsächliche Persönlichkeitsverletzung vorlag (s. zum Schadensersatzanspruch bei immateriellen Schäden auch oben Fall 9). Dafür genüge es nicht, dass der Betroffene bei einer Bank aufgrund seines Scorewerts keinen Kredit erhält, denn er könne seine Bonität der

Bank gegenüber auch anders nachweisen und im Übrigen bestehe kein Anspruch auf Vergabe eines Kredits „zu Konsumzwecken“, d. h. die Bank könnte ohnehin die Kreditvergabe (warum auch immer) verweigern.

Fall 16:
Und jetzt alle gemeinsam: Verantwortlich!

Praktischer Fall: Eine Gruppe unabhängiger Lebensmittelgroßhändler möchte eine gemeinsame Tochtergesellschaft gründen, die regelmäßig („live") Daten über die belieferten Lebensmitteleinzelhändler (Kunden) und deren Bedarf von den angeschlossenen Großhandelsunternehmen erhält und mit „big data"-Algorithmen statistisch auswertet. Es soll u. a. untersucht werden, welche Korrelationen in Bezug auf Produkte bestehen, etwa „Wer viel Salzstangen bestellt, bestellt auch viel Zitronenlimonade". Die sich aus derartigen Auswertungen ergebenden Erkenntnisse sollen sowohl (in aggregierter Form) an interessierte Dritte verkauft als auch zu konkreten Empfehlungen der gemeinsamen Tochtergesellschaft an die angeschlossenen Lebensmittelgroßhändler über erfolgversprechende „Kombinationswerbungen" gegenüber einzelnen Kunden führen.

In der datenschutzrechtlichen Theorie gibt es drei Sorten von „Kooperationen" von Stellen, die personenbezogene Daten verarbeiten. Wann eine Auftragsverarbeitung (Art. 28 DSGVO) vorliegt, ist im Detail offen (s. oben Fall 7). Das entstehende Konstrukt lässt sich aber datenschutzrechtlich als eine Beziehung zwischen einem „Herrn der Daten" (Verantwortlicher) und einem „Knecht der Daten" (Auftragsverarbeiter) darstellen. Prototyp dieser Fallgestaltung ist ein Rechenzentrumsbetreiber (Auftragnehmer), der für einen Kunden (Auftraggeber) „dessen" Daten verarbeitet.

Sind hingegen beide Stellen „Herren der Daten" und legen gemeinsam die Zwecke und die Mittel der Datenverarbeitung fest, so sind sie gemeinsam Verantwortliche (Art. 26 DSGVO). Prototyp dieser Fallgestaltung ist das gemeinsame Betreiben einer Adressdatenbank durch zwei Unternehmen.

Verfolgt hingegen jede Stelle bei einem Datenaustausch ihre eigenen Zwecke und legt ihre eigenen Mittel fest, so handelt es sich um unabhängige Verantwortliche, die sich gegenseitig Daten übermitteln (s. oben Fall 12). Prototyp dieser Fallgestaltung ist das Unternehmen, das lohnsteuerrelevante personenbezogene Daten seiner Arbeitnehmer an das Finanzamt weitergibt. Mit diesen schönen Definitionen lehnt sich so mancher Jurist, der das Thema beschreibt, zufrieden zurück: Das klingt doch alles begrifflich sehr sauber, oder?

➢ Rechtsfolgen falscher „Selbsteinschätzung“

Wie so oft beugt sich die Realität dieser Begriffsstruktur nicht ohne Weiteres. Zunächst aber noch ein kurzer Blick auf die Rechtsfolgen der Einordnung: Bei einer Auftragsverarbeitungssituation muss der Verantwortliche einen Auftragsverarbeitungsvertrag mit dem Auftragsverarbeiter abschließen, der den Kriterien des Art. 28 DSGVO genügt. Außerdem muss er die Vertragseinhaltung regelmäßig kontrollieren. Wer keine Auftragsverarbeitungsvereinbarung abschließt, obwohl eine Auftragsverarbeitungssituation vorliegt, verletzt die DSGVO. Wer alles richtig macht, erhält als Vorteil möglicherweise (s. oben Fall 7), dass er personenbezogene Daten an den Auftragsverarbeiter übertragen darf, ohne dass dafür eine eigene datenschutzrechtliche Legitimationsgrundlage gegeben sein muss (auch wenn der Auftragsverarbeiter als „Empfänger“ in Pflichthinweisen des Verantwortlichen gegenüber dem Betroffenen anzugeben ist). Denn datenschutzrechtlich werden Verantwortlicher und Auftragsverarbeiter als Einheit angesehen.

Bei einer Konstellation als „gemeinsam Verantwortliche“ muss eine Innenvereinbarung über die Verantwortlichkeitsabgrenzung abgeschlossen werden. Deren Eckdaten müssen dem Betroffenen gegenüber transparent gemacht werden, auch wenn das letztlich in der Sache völlig irrelevant ist, weil der Betroffene seine Rechte ohnehin „bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen“ kann (Art. 26 Abs. 3 DSGVO). Wer aber keine solche Vereinbarung abschließt bzw. transparent macht, obwohl eine Situation gemeinsamer Verantwortlichkeit vorliegt, verletzt die DSGVO. Wer alles richtig macht, erhält als Vorteil – nichts. Denn jede Datenübermittlung zwischen den gemeinsam Verantwortlichen bedarf einer datenschutzrechtlichen Grundlage, d. h. solche „Innenübertragungen“ sind datenschutzrechtlich nicht privilegiert. Immerhin hat das Amtsgericht Mannheim in einem Urteil vom September 2019 über einen Fall entschieden, in dem gemeinsam Verantwortliche – also ein Fall des Art. 26 DSGVO – vorlag, die aber ihr Verhältnis rechtlich falsch eingeordnet hatten und stattdessen eine Auftragsverarbeitungsvereinbarung – also eine Vereinbarung nach Art. 28 DSGVO – abgeschlossen hatten. Das Amtsgericht Mannheim war der Ansicht, dass nicht gegen Art. 26 DSGVO verstoßen wird, wenn gemeinsam Verantwortliche mit der „falschen“ Vereinbarung (insbesondere mit Regelungen zur internen Verantwortungsverteilung) nicht nur die Anforderungen des Art. 26 DSGVO, sondern darüber hinaus auch die (in dieser Konstellation irrelevanten) Erfordernisse des Art. 28 DSGVO einhalten. Das ist nicht wirklich verwunderlich, da Art. 28 DSGVO höhere Anforderungen an den Inhalt der Vereinbarung stellt, sodass in Zweifelsfällen die Einhaltung des höchsten „Standards“ ein praktikabler Weg sein könnte, um Rechtssicherheit zu erlangen.

Bei einer „gestaffelten“ Verantwortlichkeit ist hingegen zunächst nur jeder Verantwortliche für seine eigenen Verarbeitungshandlungen verantwortlich. Da aber den Empfänger von Daten ebenso Prüfpflichten hinsichtlich der „datenschutzrechtlich korrekten“ Herkunft als auch den Übermittelnden Mitteilungspflichten gegenüber dem Übermittlungsempfänger hinsichtlich bestehender (Zweck-) Einschränkungen treffen (s. oben Fall 12), werden die Verantwortlichen in der Praxis in vielen Fällen parallel bzw. gesamtschuldnerisch haften. Man darf gespannt sein, wie sich in der Praxis beispielsweise Unternehmen und Behörden, die gesamtschuldnerisch für Fehler der Verarbeitungshandlungen in Datenketten in Anspruch genommen werden, fühlen werden.

➢ Voraussetzungen gemeinsamer Verantwortlichkeit

Zurück zu den „gemeinsam Verantwortlichen“. Diese Konstruktion taucht in der DSGVO an zwei Stellen auf. Einmal wird schon der „Verantwortliche“ als solcher – wie auch schon in der EU-Datenschutzrichtlinie – definiert als jemand, der *„allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“*. Kurios ist, dass dieses „und“ von Aufsichtsbehörden immer schon als „oder“ verstanden wurde: Solange irgendeine Überschneidung bei der Festlegung des Zwecks oder (!) der Mittel vorlag, wurde eine gemeinsame Verantwortung angenommen. Schon diese, 2010 entwickelte Sichtweise schloss nur solche Fälle aus dem Begriff der „gemeinsam Verantwortlichen“ aus, in denen die Verantwortlichen jeweils „in ihrer eigenen Welt“ leben – wie ein Arbeitgeber, der Angestellte beschäftigt, und ein Finanzamt, das Steuern erhebt.

In den Entscheidungen des EuGH vom Juni 2018 (Facebook-Fanpages) und vom Juli 2019 (Like-Button) wurde gemeinsame Verantwortung sogar noch weiter definiert: Solange irgendjemandes Handeln für eine nachgelagerte Datenverarbeitung auch nur „mitursächlich“ ist, selbst wenn er selbst die Zwecke oder Mittel der Verarbeitung gar nicht (mit) festlegt, ist dieser „jemand“ im Sinne einer gemeinsamen Verantwortung mit verantwortlich (s. auch o. Fall 13). Man muss das gar nicht ironisch auf das Elektrizitätswerk überspitzen, das auch „ursächlich“ für die Datenverarbeitung bei Facebook ist, um die Tragweite dieses Gedankens herauszustellen. Insbesondere kann auf Basis dieser niedrigen Voraussetzungen eine gemeinsame Verantwortung bestehen zwischen einer Privatperson (Lockvogel, auch in Form des sog. „Youtubers“), die „irgendwie“ personenbezogene Daten Dritter „herbeischafft“, und einem Unternehmen, das diese Daten dann „irgendwie“ speichert oder sonst verarbeitet. Eine gemeinsame Verantwortung könnte auch bestehen bei Nutzung eines unternehmenseigenen Smartphones durch einen Beschäftigten, der auf dem Gerät auch private Kontakte speichert und sich mit ihnen austauscht. Die „Zeugen Jehovas“-Entscheidung des EuGH vom Juli 2018 – auch noch zur EU-Datenschutzrichtlinie – vertieft diese Grundgedanken anhand

von zwei Klarstellungen: Die Entscheidung über die Zwecke und Mittel der Verarbeitung muss nicht schriftlich fixiert sein, damit eine gemeinsame Verantwortlichkeit vorliegt. Und selbst eine Person, die aus Eigeninteresse auf die Verarbeitung durch andere Einfluss nimmt („Ermunterung"), selbst aber dann keinen Zugriff auf die personenbezogenen Daten hat, „kann" als (gemeinsam) Verantwortlicher angesehen werden.

- Gemeinsame Haftung

In der den genannten Entscheidungen des EuGH noch zugrunde liegenden EU-Datenschutzrichtlinie gab es daneben keine ausdrückliche Regelung für die Folgen der gemeinsamen Verantwortung, insbesondere also für das Innenverhältnis. In der Sache war aber bereits klar – und der EuGH sah sich nicht einmal veranlasst, das noch einmal „herzuleiten" –: Die gemeinsam Verantwortlichen haften (verschuldensunabhängig) in der Phase der gemeinsamen Verantwortlichkeit für Datenschutzverstöße des/der jeweils anderen Verantwortlichen. Wenn also Verantwortlicher A etwas „falsch" macht, kann man vom Verantwortlichen „B" verlangen, das zu unterlassen. Die ausdrückliche Regelung hierzu hat mittlerweile die DSGVO in ihrer zweiten Textstelle zur gemeinsamen Verantwortlichkeit nachgeholt (Art. 26 DSGVO). Zuvor wird aber, da die Definition des gemeinsam Verantwortlichen (s. o.) nicht genug zu sein schien, noch einmal unmissverständlich ausgeführt: *„Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche."* Die weiteren Regelungen zur gemeinsamen Verantwortlichkeit, die Art. 26 DSGVO anordnet und die bereits oben kurz wiedergegeben wurden, fokussieren sich dann auf die Innenvereinbarung zur Verantwortlichkeitsverteilung. Das Fehlen dieser Vereinbarung ist hart sanktioniert, ihr Zweck bleibt aber überwiegend im Dunkeln (Zwang zur Regelung zivilrechtlicher Innenausgleichsansprüche zwischen „datenschutzrechtlichen Gesamtschuldnern"?), da datenschutzrechtlich ohnehin „alle für alles haften".

Wenn man sich nun vor Augen hält, wer da alles so gemeinsam Verantwortlicher ist, müssen wohl noch einige Innenvereinbarungen zur Ausgestaltung der gemeinsamen Verantwortlichkeit abgeschlossen werden. Viele „betroffene Verantwortliche" werden noch gar nichts von ihrem Glück wissen, aber dennoch wird man die Situation „von außen" erkennen können (was das Risiko eines Vorgehens durch Betroffene erhöht). Besonders die Vereinbarungen zwischen Arbeitnehmern und Arbeitgebern als „gemeinsam Verantwortliche" – Stichwort „gemischt genutzte Endgeräte" – dürften den Arbeitsrechtlern noch viel Freude bereiten.

➢ Beispiel: Das „page controller addendum“ von Facebook

Auch die AGB-Rechtler stehen bei den anstehenden „Massenvereinbarungen“ (Facebook etc.) bereits in den Startlöchern und analysieren die zivilrechtliche Wirksamkeit solcher formularmäßiger Klauselwerke. Natürlich sind derartige Vereinbarungen auch nach zivilrechtlichem Maßstab zu messen. Doch das ist bislang nur ein Nebenkriegsschauplatz: Facebook veröffentlichte im September 2018 als Reaktion auf das Fanpages-Urteil des Europäischen Gerichtshofs die sog. „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“. Die Reaktion der Datenschutzkonferenz im April 2019 lautete allerdings, dass diese nicht die Anforderungen des Art. 26 DSGVO erfülle. Es stehe – neben mangelnder Transparenz – nicht im Einklang mit Art. 26 DSGVO, dass sich Facebook die alleinige Entscheidungsmacht hinsichtlich der Verarbeitung von Insights-Daten einräumen lassen wolle.

Diese Beanstandung steht in gewissem Widerspruch zur Auffassung der Datenschutzbehörden, dass „irgendeine“ Überschneidung von Zweck oder Mitteln ausreicht, um eine gemeinsame Verantwortlichkeit zu begründen: Es könnte also auch einer der Verantwortlichen nur sehr wenig außerhalb der (kleinen) Verantwortlichkeits-„Schnittmenge“ mit den Daten anstellen (wollen). Mit anderen Worten würde nach der Auffassung der Datenschutzkonferenz sogar eine (kleine) Schnittmenge zwangsläufig zu einer Verpflichtung führen, der anderen Partei seine eigenen Verarbeitungshandlungen in dieser Phase transparent zu machen und ihr Mitspracherechte in Bezug auf diese Verarbeitungshandlungen einzuräumen. Eine solche Offenlegungspflicht mag zwar in einer Situation gegenüber dem „Riesen“ Facebook sympathisch klingen, lässt sich aber Art. 26 DSGVO nicht entnehmen, wonach die gemeinsam Verantwortlichen lediglich *„in einer Vereinbarung in transparenter Form festlegen, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt“*.

Auch aus der Entscheidung des EuGH zum Facebook-Like-Button, in der zwischen den einzelnen Verarbeitungsphasen abgeschichtet wird, lässt sich keine Notwendigkeit herauslesen, dass beide Verantwortlichen im Innenverhältnis irgendeine Entscheidungsmacht behalten müssen. Dies war im Übrigen auch im Sachverhalt der Zeugen-Jehovas-Entscheidung des EuGH nicht so. Und selbst die vom Landesdatenschutzbeauftragten von Baden-Württemberg im Juni 2019 veröffentlichten Muster für eine Vereinbarung zwischen gemeinsam Verantwortlichen und für Informationen gegenüber Betroffenen scheinen solche Offenlegungspflichten nicht zu enthalten oder vorauszusetzen. Im Gegenteil: Diese Muster folgen im Grundsatz eher dem Schema „Im Innenverhältnis jeder für sich, im Außenverhältnis gemeinsamer Auftritt“.

Wie auch immer: Facebook hat im Oktober 2019 eine neue Fassung der „Ergänzung“ veröffentlicht, die die beanstandete alleinige Verfügungsmacht von Facebook nicht mehr erwähnt. Aber machen wir uns nichts vor: Die Streichung ändert an den tatsächlichen Verhältnissen – Stichwort „code as law“ – gar nichts.

Wenn man all dies zusammen nimmt, muss man wohl sagen: Die Fälle der gemeinsamen Verantwortung sind genauso ufer- wie konturenlos. Wenn das Finanzamt personenbezogene Daten der Mitarbeiter nur deshalb verarbeiten kann, weil der Arbeitgeber diese erhoben und an das Finanzamt übermittelt hat, sind nun auch diese beiden gemeinsam Verantwortliche? Im Fallbeispiel oben dürfte die Sache hingegen einigermaßen klar sein.

Fall 17:
Das „versteckte Koppelungsverbot“: Gibt es einen Vorrang der Einwilligung?

Praktischer Fall: Die Müller KG verkauft Orthopädieartikel an Endverbraucher. Frau Huber bestellt ein Paar Orthesenschuhe, die jedoch nicht auf Lager sind, sodass sie ihre Adresse hinterlässt, damit sie von der eingetroffenen Lieferung benachrichtigt werden kann. Neben einem Bestellformular mit Pflichthinweisen bezüglich der Bestellung erhält sie ein DSGVO-„Aufklärungsblatt“, aus dem sich ergibt, dass ihr Name und ihre Adresse auf Grundlage von Art. 6 Abs. 1 S. 1 lit. f) DSGVO bis auf Widerspruch zu Zwecken des Direktmarketings verarbeitet werden. Entsprechend erhält Frau Huber in den Folgejahren regelmäßig Kataloge der Müller KG zugesandt.

In diesem Fall geht es nicht (wie oben in Fall 8) um die Frage, wie lange personenbezogene Daten zu Direktmarketingzwecken verarbeitet werden dürfen. Es geht auch nicht darum, eine „parallele“ Legitimation in zwei Grundlagen zu sehen, also eine datenschutzrechtliche Rechtfertigung „auf zwei Beine“ zu stellen (auch dazu s. oben Fall 8). Vielmehr geht es um die Frage des Verhältnisses von zwei Legitimationsgrundlagen für die komplementären Zwecke A (hier: Verkauf) und B (hier: Direktwerbung).

➢ Eingabeformulare und Pflichthinweise

Was das Bestellformular mit Pflichthinweisen angeht, hat die Müller KG schon einmal etwas richtig gemacht. Der Thüringer Landesbeauftragte für Datenschutz schreibt in seinem Tätigkeitsbericht 2018 zur Lokalisierung von Pflichtinformationen bei Formularen:

„Werden die personenbezogenen Daten beispielsweise mit einem schriftlichen oder elektronischen Formular erhoben, müssen die Informationen grundsätzlich auf diesem Formular bereitgestellt werden.“

➢ Zweckbindung bei Verträgen

Aus der verhältnismäßig engen Zweckbindung der DSGVO ergibt sich – so wurde das Datenschutzrecht auch schon immer interpretiert –, dass bei Bestehen eines Vertrags die Daten des Vertragspartners nur für die Zwecke der Durchführung des Vertrags verarbeitet werden dürfen (Art. 6 Abs. 1 S. 1 lit. b) DSGVO). Einfach gesagt: Wer einem Kunden etwas verkauft,

darf die personenbezogenen Daten dieses Kunden nicht dafür benutzen, Werbung zu betreiben. Das klingt einleuchtend, wird aber in der Praxis häufig ignoriert und neuerdings auch – weil man sonst allen Unternehmen Bußgeldbescheide schicken müsste? – von den Datenschutzbehörden etwas aufgeweicht (s. unten Fall 29).

Auch hier kann man aber schon die Frage stellen, wo genau die Erforderlichkeit der Verarbeitung für die Erfüllung des Vertrags endet, Stichwort Buchhaltung/Rechnungslegung/Jahresabschluss (s. dazu auch oben Fall 7). Der Europäische Datenschutzausschuss stellt in seinen Empfehlungen vom April 2019 sogar ausdrücklich klar, dass etwa die „Heimadresse" nicht mehr mit der Verarbeitung zu Vertragszwecken gerechtfertigt werden kann, wenn eine Abholstation als Lieferort gewünscht ist:

„However, if the customer has opted for shipment to a pick-up point, the processing of the data subject's home address is no longer necessary for the performance of the purchase contract and thus a different legal basis than Article 6(1)(b) is required."

Ob für die Erhebung und Speicherung der Privatadresse eine „andere Rechtsgrundlage" („*different legal basis*") als der Vertrag gefunden werden kann, dürfte dann zweifelhaft sein.

Ähnliches würde im Übrigen auch gelten, wenn es sich um ein Produkt handelt, das digital „ausgeliefert" wird. In diesem Fall dürfte nach einem Beispielssachverhalt in den Empfehlungen des Europäischen Datenschutzausschusses vom November 2019 zum Thema „*privacy by design/by default*" nicht einmal die Adresse erhoben werden (bevor man das unterlässt, sollte man allerdings besser noch einmal mit einem Umsatzsteuerrechtler Rücksprache halten, ob nicht doch eine Rechnungsadresse des Empfängers benötigt wird):

„Moreover, there are situations where an address will not be necessary. For example, when ordering an eBook the customer can download the product and his or her address does not need to be processed by the webshop. The webshop owner therefore decides to make two web forms: one for ordering books, with a field for the customer's address and one web form for ordering eBooks without a field for the customer's address."

Unabhängig aber von der Frage, was genau für den Vertragsabschluss bzw. die Vertragsabwicklung „erforderlich" ist, lässt sich hinsichtlich der Ansprache von „Marktteilnehmern" mithilfe von „Vertragsdaten" zumindest sagen, dass das Wettbewerbsrecht etwas weniger streng „zweckgebunden" ist. Für postalisch adressierte Werbung gleich welchen Inhalts gilt

letztlich ein „opt-out“ – solange nicht „*erkennbar ist, dass der angesprochene Marktteilnehmer diese Werbung nicht wünscht*“ (§ 7 Abs. 1 S. 2 UWG), ist sie im Grundsatz zulässig. Wer dagegen eine E-Mail-Adresse eines Kunden im Zusammenhang mit dem Verkauf von Waren oder Dienstleistungen erhalten hat, darf dem Kunden immerhin Werbung „*für eigene ähnliche Waren oder Dienstleistungen*“ schicken, solange der Kunde darauf hingewiesen wurde, dass er der Verwendung jederzeit widersprechen kann und der Kunde bislang nicht widersprochen hat (§ 7 Abs. 3 UWG). Datenschutzrechtlich aber ist Direktmarketing ein anderer Zweck als der ursprüngliche Vertragszweck, der hier nur in einem Kauf besteht. Genauer wird unten in Fall 29 auf diese wettbewerbsrechtlichen Grundsätze eingegangen.

- Doppelter Zweck

Das Überschreiten der ursprünglichen Zweckgrenze (Kauf) lässt sich nun gedanklich scheinbar auf zwei Weisen lösen: Entweder man verwendet die Daten zu einem anderen Zweck als ursprünglich erhoben, dann muss ein Zweck-Kompatibilitäts-Test durchgeführt werden (Art. 6 Abs. 4 DSGVO) und der Kunde muss über den neuen Zweck benachrichtigt werden (Art. 13 Abs. 3 DSGVO). Schon dies wirft die Frage auf, ob für Vertragszwecke erhobene Daten bereits „eine logische Sekunde“ nach ihrer Erhebung in Richtung Direktmarketing „zweckverändert“ werden können; denn eigentlich beabsichtigte der Verkäufer ja schon im Moment der Erhebung, die Daten auch zu Werbezwecken zu verwenden. Es liegt daher eigentlich gar keine Zweckänderung, sondern von vornherein ein „Doppelzweck“ vor. Ohnehin bestehen Zweifel, ob der Zweck-Kompatibilitäts-Test hier erfolgreich wäre. Der Europäische Datenschutzausschuss hat in seinen Empfehlungen vom April 2019 – zumindest im Kontext von Dauerschuldverhältnissen – (ohne weitere Diskussion der Rechtsgrundlagen) ausgeführt:

„*Where processing of personal data is based on Article 6(1)(b) and the contract is terminated in full, then as a general rule, the processing of that data will no longer be necessary for the performance of that contract and thus the controller will need to stop processing. The data subject might have provided their personal data in the context of a contractual relationship trusting that the data would only be processed as a necessary part of that relationship. Hence, it is generally unfair to swap to a new legal basis when the original basis ceases to exist.*“

Ob dies auch für punktuelle Austauschverträge wie einen Kaufvertrag gilt, erläutern die Empfehlungen nicht weiter.

Geht man hingegen davon aus, dass der zweite Zweck – die Verwendung zum Betreiben von Direktmarketing – bereits von Anfang an besteht, so bestimmt Erwägungsgrund 47 „gesetzesgleich", dass *„die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden kann"*. Es wäre also zulässig, die Daten von Anfang an „nur" zu Direktmarketingzwecken zu erheben und dies datenschutzrechtlich mit dem Direktmarketinginteresse zu legitimieren. Entsprechende Transparenz – sprich Pflichtinformationen – gegenüber dem Kunden vorausgesetzt, scheint es so, als könne man die Daten „auf zwei komplementären Säulen" erheben: einmal für den Vertrag bzw. dessen Durchführung (Art. 6 Abs. 1 S. 1 lit. b) DSGVO), einmal für Direktmarketingzwecke (Art. 6 Abs. 1 S. 1 lit. f) DSGVO).

In diese Richtung geht auch die „Orientierungshilfe" der Datenschutzkonferenz zum Thema Direktwerbung vom November 2018: Daten, die im Rahmen einer Geschäftsbeziehung (d. h. zu vertraglichen Zwecken) erhoben wurden, können „grundsätzlich" (daneben) für E-Mail-Werbung verwendet werden, wenn dieser Zweck *„den betroffenen Personen bei Datenerhebung transparent dargelegt worden ist"* und die wettbewerbsrechtlichen Vorgaben eingehalten werden. Mit den dabei betroffenen Fragen der Interessenabwägung selbst (und dem Verhältnis zu den wettbewerbsrechtlichen Vorgaben) beschäftigt sich Fall 29 unten. Umgekehrt ausgedrückt – so auch die Datenschutzkonferenz – können personenbezogene Daten, die ursprünglich nicht (auch) zu Zwecken der Werbung erhoben wurden, nur für Werbezwecke verwendet werden, wenn die Regelungen über die Zweckänderung (s. o.) eingehalten werden.

➢ Vorrang der Einwilligung bei „Anwesenheit" des Betroffenen?

Dem kritischen Leser schießt nun natürlich ein Gedanke durch den Kopf: Wenn der Betroffene ohnehin schon dabei ist, einen Vertrag abzuschließen, wenn er also „präsent" bzw. „am Draht" ist, dann könnte man ihn ja auch gleich nach seiner Einwilligung fragen, ob er (neben dem Vertrag) mit Direktmarketing an ihn einverstanden ist. Man könnte diesen Gedanken als „Vorrang der Einwilligung" bezeichnen, obwohl oft betont wird, dass die verschiedenen datenschutzrechtlichen Legitimationsgründe gleichberechtigt nebeneinander stehen. Nun möchte aber ein typischer Verantwortlicher keine eigenständige Einwilligung für Direktwerbungszwecke einholen, denn eine Einwilligung („opt-in" bzw. „Haken setzen") werden viel weniger Betroffene erteilen wollen als später Betroffene Widerspruch gegen die Verarbeitung zu Direktwerbungszweck erheben werden („opt-out", Art. 21 Abs. 2 DSGVO). Ein „Geschmäckle" scheint die Sache aber dennoch zu haben: Immerhin offenbart der Betroffene seine Kontaktdaten aus seiner Sicht nur zu dem Zweck, einen Vertrag abzuschließen. Wenn man ihn nur gefragt hätte, ob er seine Daten auch zu Werbezwecken „hergibt",

hätte er vielleicht „nein“ gesagt. Von daher ist das künstliche „Aufpfropfen“ eines – für sich genommen legitimen – zweiten Verarbeitungszwecks vielleicht doch nicht so unproblematisch?

Bereits die Kommentarliteratur zum alten Datenschutzrecht war der Meinung, dass „die unmittelbare Anfrage bei den Betroffenen dem mittelbaren Zugang vorgeht“. Das Verwaltungsgericht Bayreuth hat dies in einer (lesenswerten) Entscheidung vom 8. Mai 2018, zwischenzeitlich vom Bayerischen Verwaltungsgerichtshof bestätigt, bekräftigt. Eine Interessenabwägung als Grundlage – immerhin handelt es sich ja der Sache nach um eine „mutmaßliche Einwilligung“ (s. oben Fall 8) – komme erst in Betracht, wenn eine Mitwirkung des Betroffenen ausscheidet. Das Verwaltungsgericht Bayreuth fügt an, wenn man die Daten im Rahmen von Bestellvorgängen erwirbt, sei es ohne unverhältnismäßig großen Aufwand möglich, im Einzelfall eine Einwilligung einzuholen. In den DSGVO-Kommentierungen kommt dieser Gedanke des „Vorrangs der Einwilligung“ bislang so gut wie gar nicht vor.

Juristischer Dreh- und Angelpunkt ist dabei übrigens das Wörtchen „erforderlich“, dessen Interpretation an vielen Stellen des Datenschutzrechts Kopfschmerzen bereitet. Eine Datenverarbeitung auf Basis einer Interessenabwägung ist nur dann zulässig, wenn die Verarbeitung zur Erreichung des in die Abwägung eingestellten Interesses des Verantwortlichen „erforderlich“ ist. Man kann dies – mit dem Verwaltungsgericht Bayreuth – so lesen, dass eine auf Interessenabwägung gestützte Verarbeitung solange nicht „erforderlich“ ist, wie der Verantwortliche sein Informationsziel anders, insbesondere durch eine Einwilligung, erreichen kann. Im Wort „erforderlich“ steckt dann die Nachrangigkeit der Interessenabwägung gegenüber der Einwilligung – die Gleichberechtigung der verschiedenen Legitimationsgründe wäre also dahin.

➢ Das Verhältnis zum Wettbewerbsrecht

In der Praxis würde dies dazu führen, dass die DSGVO eine Fallgestaltung verbietet, die das Wettbewerbsrecht – wie oben skizziert – erlaubt. Selbst für E-Mail-Adressen, die ein Unternehmen „im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von einem Kunden erhalten hat“, geht der (deutsche) Gesetzgeber davon aus, dass die Wiederholungsansprache dieses Kunden für „*eigene ähnliche Waren oder Dienstleistungen*“ gerechtfertigt ist und der Kunde dazu nicht extra befragt werden muss (s. o.). Es bedarf also keines „opt-ins“ (Einwilligung), sondern nur des Hinweises auf die „opt-out“-Möglichkeit. Nach der DSGVO würde hier aber, wenn man die althergebrachte datenschutzrechtliche Interpretation unterstellt, der „Vorrang der Einwilligung“ gelten, d. h. der Kunde muss „den Haken aktiv setzen“.

Das Verhältnis zwischen Wettbewerbsrecht – § 7 UWG basierte übrigens auf der „E-Privacy-Richtlinie“ der EU, die eigentlich schon längst durch die E-Privacy-Verordnung hätte abgelöst werden sollen – und DSGVO ist ohnehin unklar. Die „Orientierungshilfe“ der Datenschutzkonferenz zum Thema Direktwerbung vom November 2018 ist der Ansicht, dass die Wertungen des UWG (im Rahmen der Interessenabwägung) in die DSGVO „hineinzulesen“ sind, also: Etwas, das wettbewerbsrechtlich erlaubt oder nicht erlaubt ist, sollte auch datenschutzrechtlich entsprechend zulässig oder verboten sein. Danach sollte es also eigentlich keine Abweichungen zwischen beiden Ebenen geben. Dass dies aber zumindest nicht uneingeschränkt gilt, zeigt Fall 29.

➢ Vorrang der Interessenabwägung bei unbekannter Identität?

Einen vor diesem Hintergrund interessanten „Twist“ enthält nun die „Orientierungshilfe für Anbieter von Telemedien“ der Datenschutzkonferenz vom März 2019, wonach im Bereich von Tracking-Maßnahmen im Internet (Cookies etc.) der Vorrang der Interessenabwägung vor der Einwilligung mit einem ganz anderen Argument in Betracht gezogen wird: Um eine Einwilligung einzuholen und nachweisbar vorzuhalten, müsste der Webseiten-Betreiber mehr Daten erheben – nämlich die Identifizierung des Einwilligenden auf Einzelnutzerebene – als im Rahmen einer Interessenabwägung notwendig sind. Das datenschutzrechtliche Gebot der Datensparsamkeit rückt dabei in den Vordergrund. Wer nur die (pseudonymen) Daten von „identifizierbaren“ Betroffenen in Form von Geräte-IDs verarbeitet (genaugenommen natürlich nur solche, die bestimmten „Endgeräten“ zugewiesen sind, denn welche Person davor sitzt, kann nur durch Kombination mit weiteren Daten ermittelt werden), der sollte nicht mit dem Argument einer sicher beweisbaren Einwilligung den Betroffenen auch noch genau fragen, wer er eigentlich ist, und damit noch mehr Daten sammeln. Die Frage, wann die Erhebung zusätzlicher Daten in derartigen Konstellationen nicht notwendig ist, wird unten in Fall 39 noch eingehender erörtert. Die Orientierungshilfe präferiert jedenfalls auf der Ebene des Legitimationsgrunds selbst eine nur typisierte Interessenabwägung, die zu einer mutmaßlichen Einwilligung führt, selbst wenn der Betroffene dem Webseiten-Betreiber eigentlich virtuell „gegenübersitzt“ und auch nach seiner Einwilligung gefragt werden könnte (obwohl die Datenschutzbehörden im Zusammenhang mit der Interessenabwägung in anderen Zusammenhängen gerade auf einer dokumentierten Einzelfallentscheidung beharren).

Die Doppelzüngigkeit dieser Vorgabe wird allerdings in der Literatur so beschrieben: *„Hinter der Subsidiarität der Einwilligung mag auch die Sorge stehen, dass Datenschutz als Folge*

des unbesehenen Wegklickens von massenhaft abgefragten Einwilligungen von den betroffenen Personen zunehmend als lästige Förmelei wahrgenommen wird und mit der Datenschutz-Ermüdung die gesellschaftliche Akzeptanz schwindet".

Man kann dies wie folgt zusammenfassen: Kennt der Verantwortliche die Identität des Betroffenen bereits und besteht mit diesem direkter Kontakt, kann es sein, dass die Einwilligung Vorrang genießt. Kennt der Verantwortliche nur ein Pseudonym des Betroffenen – was in aller Regel gleichwohl zu einer Zurechnung der Zuordnungsinformation zum Verantwortlichen führt (s. die in der Einleitung behandelten gerichtlichen Entscheidungen zur dynamischen IP-Adresse) –, so dürfte die Interessenabwägung Vorrang genießen, denn ansonsten muss ausschließlich für eine beweisbare Einwilligung die „wahre" Identität erfragt werden, was gegen den Grundsatz der Datenminimierung verstoßen würde. Man darf gespannt sein, bei welcher internen Datenschutzdokumentation eines Verantwortlichen man dazu Ausführungen lesen kann.

Im Falle von Cookies – also von Textdateien, die der Browser des Benutzers auf „Anweisung" des Webseiten-Betreibers auf den Massenspeicher des Benutzers schreibt – ist allerdings ergänzend auf das Urteil des Europäischen Gerichtshofes vom Oktober 2019 in der Sache „Planet 49" hinzuweisen. Dieses Urteil relativiert die „Orientierungshilfe für Anbieter von Telemedien" der Datenschutzkonferenz vom März 2019, was das Setzen von Cookies angeht, denn hierfür gilt nicht (nur) das Datenschutzrecht, sondern folgende Regelung der EU-„Datenschutzrichtlinie für die elektronische Kommunikation" (e-Privacy-Richtlinie):

„Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann."

In diesem Fall ist also, wie der Europäische Gerichtshof klargestellt hat, für das Schreiben und Lesen von Daten auf Geräten des Benutzers eine „Einwilligung" erforderlich, und zwar – gemäß Art. 4 Nr. 11 DSGVO – eine aktive Handlung (s. dazu auch oben Fall 8). Eine

Interessenabwägung (mutmaßliche Einwilligung) reicht nicht aus, um diesen „Hardwarezugriff“ auf das „Benutzereigentum“ zu rechtfertigen. Nicht das Datenschutzrecht – der Schutz von personenbezogenen Daten des Betroffenen – gibt also im Bereich der Cookie-Fälle den schärfsten Maßstab vor, sondern der Schutz der „informationellen Integrität des Endgeräts“, sprich: Fernzugriffe auf die lokal gespeicherten Daten des Benutzers. Dass die oben zitierte Regelung mit „Vertraulichkeit der Kommunikation“ überschrieben ist, kann nicht darüber hinwegtäuschen, dass die Speicherung von (irgendwelchen) Informationen im Endgerät des Teilnehmers bzw. Nutzers keine Kommunikation ist, deren Vertraulichkeit zu schützen ist, sondern – ohne entsprechende Aufklärung – ein „heimlicher“ Zugriff auf fremde Hardware (Besitzstörung).

Fall 18:
Die Privatperson als Verantwortlicher

Praktischer Fall: Herr Müller ist Initiator einer Whatsapp-Gruppe mit ca. 15 Personen. Es handelt sich um den „virtuellen Stammtisch" von einigen Mitgliedern des örtlichen Kegelvereins. Die Mitglieder der Gruppe tauschen sich gegenseitig über ihre Aktivitäten und die Aktivitäten ihrer Familien, über Dritte, über Geburtstage, Krankheiten und sonstige Umstände aus. Die Huber AG, ein Hersteller von Kegelsport-Ausrüstungen, erfährt von der Existenz der Whatsapp-Gruppe und fragt bei Herrn Müller an, ob sie ihre Produkte gegenüber den Mitgliedern der Whatsapp-Gruppe bewerben könne. Herr Müller erhält von der Huber AG eine „exquisite Kegelausrüstung" und gibt die ihm bekannten Kontaktdaten der Gruppenmitglieder an die Huber AG weiter mit der Auflage, dass die Herkunft der Daten nicht offengelegt werden darf.

Es wurde bereits darauf hingewiesen, dass eine Privatperson und ein Unternehmen „gemeinsam Verantwortliche" sein können, sodass zwischen ihnen eine Innenvereinbarung nach Art. 26 DSGVO abgeschlossen werden muss (s. o. Fall 16). Das setzt natürlich voraus, dass die Privatperson überhaupt „Verantwortlicher" sein kann. Die DSGVO findet nämlich insgesamt keine Anwendung auf eine Verarbeitung personenbezogener Daten „zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten" (Art. 2 Abs. 2 lit. c) DSGVO). Man bezeichnet diese Regelung auch als „Haushaltsausnahme" (s. o. Fall 1). Zum typisch persönlichen bzw. familiären Bereich gehören Freizeit, Urlaub, privater Konsum oder Sport, also alles, was keinen Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit aufweist. Persönlicher oder familiärer Schriftverkehr sowie Anschriftenverzeichnisse sollen – so Erwägungsgrund 18 – selbst dann hierunter fallen, wenn dafür soziale Netze genutzt werden oder diese Tätigkeiten online verrichtet werden. Es scheint also datenschutzrechtlich – was natürlich schon als „zu weit" kritisiert wurde – eine Art „öffentliche Privatsphäre" zu geben, innerhalb derer die Zurschaustellung personenbezogener Daten nicht der DSGVO unterfällt, solange sie ausschließlich privaten Zwecken dient. Bei einer „Mischnutzung" von personenbezogenen Daten auch für berufliche Zwecke führt das Wort „ausschließlich" hingegen zur Anwendbarkeit der DSGVO und damit zur Verantwortlicheneigenschaft der Privatperson. Liest man einen Zeitungs- oder Fachartikel nun beruflich oder „ausschließlich" privat (s. o. Fall 1)?

Die Frage, wo dieses Haushalts-„Privileg" genau endet, ist damit von großer Relevanz. Immerhin geht es um ein großes „Pflichtenpaket" für den Verantwortlichen, wenn die DSGVO erst einmal „zuschlägt". Früher wurde vertreten, dass, sobald der „öffentliche Raum" betreten

wird, keine private bzw. familiäre Tätigkeit mehr gegeben sein kann. Familienbilder auf Facebook, die von jedermann angesehen werden können, ein privater Blogeintrag auf einer Website, eine Drohne, die auch öffentlichen Straßenraum filmt: In solchen Fällen sollte kein ausreichendes Maß an „Privatheit" mehr vorliegen. Wenn nun „privater Schriftverkehr" in sozialen Netzen öffentlich sichtbar ist oder „Anschriftenverzeichnisse" öffentlich einsehbar „online gestellt" werden, liegt nach herkömmlichem Begriffsverständnis „eigentlich" keine persönliche bzw. familiäre Tätigkeit mehr vor, auch wenn der „gesetzesgleiche" Erwägungsgrund 18 dieses herkömmliche Begriffsverständnis nicht teilt. Was ist nun mit den ganzen Live-Video-übertragenden Computerspielern, den Facebook-Junkies, Twitter-Königen, Instagram-Jüngern und „Youtubern", die ihre Privatsphäre öffentlich zur Schau stellen und damit Aufmerksamkeit, „Klicks" und irgendwann Einkommen generieren? Darf man als Hobby-Fotograf in europäischen Städten Fotos machen, auf denen Einwohner abgebildet sind?

Ein wesentlicher Punkt in diesem Zusammenhang ist das „Aufschwingen" zum Verantwortlichen, wenn die Grenzen des Persönlichen bzw. Familiären gesprengt werden, so wie auch ein Auftragsverarbeiter, wenn er sich zum Verantwortlichen „aufschwingt", zum Verantwortlichen wird (Art. 28 Abs. 10 DSGVO). Selbst wenn Erwägungsgrund 18 extra festhält, dass die DSGVO natürlich für diejenigen Verantwortlichen gilt, „die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen" – hier also Whatsapp –, dient doch Herr Müller zunächst als „Lockvogel", um Whatsapp analysefähige personenbezogene Daten der anderen Teilnehmer (inklusive deren Adressbuchinhalten) zuzuführen. Das würde, wenn man die Facebook-Entscheidung des EuGH daneben legt (s. o. Fall 16), gegen das Vorliegen der „Haushaltsausnahme" und für eine Stellung als gemeinsam Verantwortliche zwischen Whatsapp und Herrn Müller sprechen. Allerdings erhält Herr Müller nichts für dieses „Zuführen" zu wirtschaftlichen Zwecken von Whatsapp; aus seiner Perspektive steht der persönliche Austausch mit Bekannten im Vordergrund. Oder „erhält" Herr Müller eine Messaging-Plattform von Rang „unentgeltlich" als Gegenleistung zur Verfügung gestellt, so wie der Fanpage-Betreiber von Facebook eine Social-Network-Plattform (mit ihren Gestaltungsmöglichkeiten und der Sogwirkung ihrer Marke) von Rang „unentgeltlich" zur Verfügung gestellt bekommt? Bei einem anderen Messaging-Plattform-Betreiber müssten vielleicht sämtliche Teilnehmer erst eine App kostenpflichtig erwerben, was der eine oder andere vielleicht nicht wollen würde, weshalb ja das Modell „Daten gegen Geld" so attraktiv geworden ist.

Spätestens aber beim „Deal“ mit der Huber AG werden die persönlichen Kontaktdaten endgültig „kommerzialisiert“. Sie stellen eine Gegenleistung von Herrn Müller für den Erhalt seiner geldwerten Ausrüstung dar. Hier ist es deutlicher, dass sich Herr Müller zum Verantwortlichen, der Daten wohl datenschutzwidrig „übermittelt“, aufschwingt. Herr Müller hätte also den anderen Teilnehmern zumindest Zweckänderungs-Pflichthinweise (Art. 13 Abs. 3 DSGVO) zukommen lassen müssen. Und er müsste natürlich auch ein Verarbeitungsverzeichnis anfertigen müssen, sofern er „nicht nur gelegentlich“ personenbezogene Daten verarbeitet. Vielleicht sollte er auch über technisch-organisatorische Maßnahmen nachdenken.

Gegen Privatpersonen, die Verantwortliche im Sinne der DSGVO sind, richten sich übrigens sämtliche Sanktionen bei Datenschutzverstößen, die sich auch gegen Unternehmen richten könnten. Doch halt: Im Unterschied zu Unternehmen darf hier von einer Geldbuße abgesehen werden. Der „gesetzesgleiche“ Erwägungsgrund 148 erklärt dazu ausdrücklich, dass, „falls eine voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde“, anstelle einer Geldbuße auch eine Verwarnung erteilt werden kann. Immerhin.

Fall 19:
Der Headhunter und die Gehaltshöhe

Praktischer Fall: Herr Schulze ist Headhunter seiner Ein-Mann-GmbH „Schulze Headhunting GmbH". Im Auftrag der Huber AG sucht Herr Schulze eine(n) leitende(n) Angestellte(n) im Bereich Vertrieb. Für den Fall einer erfolgreichen Einstellung, so wird vereinbart, erhält die „Schulze Headhunting GmbH" eine Erfolgsprovision, deren Höhe vom (Anfangs-) Gehalt des/der neuen Mitarbeiters/in abhängig ist. Herr Schulze identifiziert Frau Müller, mit der er verschiedene Gespräche für einen Auftraggeber führt, „der zunächst anonym bleiben möchte", und die danach Gespräche mit der Personalabteilung der Huber AG führt. Frau Müller wird von der Huber AG eingestellt zu einem bis kurz vor Vertragsunterzeichnung verhandelten (Anfangs-) Gehalt. Die Huber AG teilt daraufhin Herrn Schulze das Gehalt von Frau Müller mit, woraufhin Herr Schulze der Huber AG die Provision in Rechnung stellt.

Wie in Fall 7 stellt sich hier zunächst die Frage der Reichweite des § 26 BDSG, der vorgibt: *„Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies [...] nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung [...] erforderlich ist*". Nun ist eine Mitteilung des Gehalts an einen vor Abschluss des Beschäftigungsverhältnisses im Auftrag des (späteren) Arbeitsgebers tätigen Headhunter aber wohl nicht zur Durchführung des Anstellungsverhältnisses „erforderlich".

Auch Art. 6 Abs. 1 S. 1 lit. b) DSGVO kommt als Legitimationsgrund nicht infrage, wenn man auf den Dienstvertrag der Huber AG mit dem Headhunter abstellen wollte. Denn es handelt sich nicht um einen Vertrag, „dessen Vertragspartei die betroffene Person ist", und Frau Müller hat keinen Vermittlungsvertrag mit der „Schulze Headhunting GmbH" abgeschlossen. Auch ist die Weitergabe des Gehalts nicht „zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen", weil die Mitteilung bzw. Bestätigung der Gehaltshöhe (datenschutzrechtlich: die Verarbeitung der personenbezogenen Daten) erst nach dem Vertragsabschluss stattfindet.

Dasselbe Ergebnis gilt für Art. 6 Abs. 1 S. 1 lit. c) DSGVO, was man allerdings erst merkt, wenn man diesen im Zusammenhang mit Art. 6 Abs. 2 und 3 DSGVO liest: Zwar unterliegt die Huber AG als Verantwortliche einer „rechtlichen Verpflichtung" aus dem Dienstvertrag, dem Headhunter das Gehalt mitzuteilen, aber mit „rechtliche Verpflichtung" ist hier aus-

schließlich eine gesetzliche Verpflichtung gemeint. Es ist wohl nur sehr erleuchteten Personen in Brüssel verständlich, weshalb die ursprünglich im Kommissions- und Parlamentsentwurf verwendete Formulierung „gesetzliche Verpflichtung“ derart verschlimmbessert wurde.

Häufig werden dennoch in der Praxis Gehälter bedenkenlos – und ohne Wissen des Betroffenen – an den Headhunter weitergegeben. Mit einer freiwilligen Einwilligung des Betroffenen wäre das natürlich kein Problem. Ob eine solche Einwilligung im Beschäftigungsverhältnis freiwillig gegeben werden kann, bestimmt sich nach § 26 Abs. 2 BDSG. Dort heißt es so schön: „Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen.“ Dabei ist schon die Verwendung des Wortes „insbesondere“ Fluch und Segen zugleich. In der Praxis wird sich vermutlich kein Arbeitgeber auf andere Fallkonstellationen der Freiwilligkeit der Arbeitnehmereinwilligung als die hier ausdrücklich genannten sicher verlassen wollen, auch wenn „insbesondere“ bedeutet, dass es noch andere Fälle geben könnte – zu „sperrig“ sind die beiden aufgezählten Beispiele. Rechtliche oder wirtschaftliche Vorteile für Frau Müller werden sich aus ihrer Einwilligung wohl nicht ergeben. So trifft sie keine Pflicht, bei Verweigerung den Headhunter aus eigener Tasche zu zahlen. Und ob Frau Müller das Interesse „verfolgen sollte“, dass der Headhunter sein Geld erhält, aber dabei auch ihre Gehaltshöhe erfährt, erscheint wenig plausibel.

Was vordergründig bleibt, wenn nichts anderes hilft, ist wieder einmal die Interessenabwägung, verbunden mit dem in Fall 17 geschilderten Problem, ob man nicht Frau Müller fragen muss, wenn sie schon ohnehin ihren Anstellungsvertrag mit dem Verantwortlichen unterschrieben hat und ohne Mühen „greifbar“ ist – mit der zusätzlichen Schwierigkeit, dass das vielleicht nichts bringen würde, weil ihre Einwilligung nicht als freiwillig einzustufen wäre.

Aber ungeachtet dessen: Wohin führt die Interessenabwägung? Man könnte es kurz halten und sagen, dass es natürlich zur Wahrung des berechtigten Interesses „eines Dritten“, also der „Schulze Headhunting GmbH“, erforderlich ist, dass die Gehaltshöhe durch den Verantwortlichen Huber AG mitgeteilt wird. Anonymisieren kann man die Daten auch nicht; Herr Schulze weiß ja, wen er vermittelt hat. Oder sollte am Ende noch das Datenschutzrecht die Möglichkeiten zur Strukturierung des Entgelts einschränken, dessen Ermittlung hier nun einmal personenbezogene Daten – die Gehaltshöhe – als Bezugsgröße benötigt? Da könnte ja jeder kommen. Interessant bleibt dann noch die Frage, welche „Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen“ könnten.

Ungeachtet dieser letzten Frage wäre Frau Müller gegenüber die Weitergabe ihrer Gehaltshöhe an den Headhunter vorab anzukündigen, weil die Daten gerade nicht für Zwecke ihres Beschäftigungsverhältnisses übermittelt werden sollen (Art. 13 Abs. 3 DSGVO). Frau Müller könnte dann „eskalieren" und Widerspruch einlegen (Art. 21 Abs. 1 DSGVO) „aus Gründen, die sich aus ihrer besonderen Situation ergeben". Was immer das für Gründe sind: Bis „feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen", kann Frau Müller die Einschränkung der Verarbeitung verlangen (Art. 18 DSGVO).

Während dieser Phase darf die Huber AG die Daten jedoch immerhin noch „verarbeiten" – also auch an die „Schulze Headhunting GmbH" übermitteln –, und zwar entweder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder aber zum Schutz der Rechte einer anderen natürlichen oder juristischen Person (Art. 18 Abs. 2 DSGVO). Wenn nun also die „Schulze Headhunting GmbH" die Huber AG rechtlich auf Auskunft über die Gehaltshöhe (als Faktor für die Entgeltermittlung) „in Anspruch nimmt" (was immer das heißt – reicht ein Anwaltsschreiben?), darf dann die Huber AG während der Phase der eingeschränkten Verarbeitung die Gehaltshöhe doch „zur Verteidigung von Rechtsansprüchen" mitteilen? Gemeint ist hier übrigens von der DSGVO wohl eher die Verteidigung „gegen" Rechtsansprüche. Oder ist alternativ die Mitteilung an die „Schulze Headhunting GmbH" zum Schutz von deren (vertraglichen) Rechten zulässig, weil diese Übermittlung, wie die Kommentarliteratur weiter definiert, auch unter Abwägung der Rechte der Betroffenen „unbedingt notwendig" ist?

Fall 20:
Direktmarketing gegenüber Unternehmensrepräsentanten oder gegenüber Unternehmen?

Praktischer Fall (Beginn wie Fall 1): Herr Müller, Einkäufer der Huber AG, übergibt einem Vertriebsmitarbeiter der Maier GmbH, Herrn Schulze, eine Visitenkarte von sich mit den Worten „Wenn Sie mal das Produkt X in Richtung Y weiterentwickeln, dann rufen Sie mich an". Die Maier GmbH entwickelt in der Folgezeit das Produkt X in Richtung Y weiter. Herr Schulze ruft Herrn Müller an, woraufhin die Huber AG das weiterentwickelte Produkt der Maier GmbH einer intensiven Evaluierung unterzieht, ob dieses von der Huber AG als Teil eines ihrer eigenen Produkte bezogen werden soll. In dieser Phase telefonieren Herr Schulze und Herr Müller häufiger miteinander und unternehmen zudem, da sie beide passionierte Segler sind, mit ihren Familien einen gemeinsamen Segelausflug. Während dieser Phase verlässt Herr Schulze die Maier GmbH und wechselt zu einem potentiellen Abnehmer der Produkte der Huber AG, der Lehmann KG. Einige Monate nach diesem Wechsel ruft Herr Müller Herrn Schulze an und erzählt ihm, dass die Huber AG das weiterentwickelte Produkt der Maier GmbH nicht weiter verfolgt habe. Herr Müller zeigt sich jedoch von der Marktabdeckung der Lehmann KG angetan und fragt Herrn Schulze, ob die Lehmann KG nicht Interesse daran hätte, Produkte der Huber AG zu vertreiben.

Dieser Fall baut auf der in Fall 1 behandelten Fragestellung auf, ob die „Übermittlung" von unternehmensbezogenen Kontaktdaten eines Repräsentanten eines Unternehmens (hier der Huber AG) zu einem „Erheben" aufseiten des anderen Unternehmens (hier der Maier GmbH) führt. Wer diese Frage bejaht und ein Erheben immer annimmt, wenn personenbezogene Daten in die „Sphäre" eines Verantwortlichen gelangen, egal wie und warum, muss sich zwar mit den Folgen beschäftigen (Pflichthinweise nach Art. 13 und 14 DSGVO), kann aber den vorliegenden Fall weitgehend ignorieren.

In Fall 1 wird unterstellt, dass sich der Zweck der Übermittlung der Kontaktdaten des Repräsentanten des übermittelnden Unternehmens sowie das Interesse des empfangenden Unternehmens auf die Eigenschaft des Repräsentanten als „Funktionsträger" beschränkt. Danach wäre es also der Huber AG völlig gleichgültig, ob der Vertriebsmitarbeiter der Maier GmbH Herr Schulze oder Herr Sowieso heißt, und der Maier GmbH völlig gleichgültig, ob der Einkäufer der Huber AG nun Herr Müller oder Herr Sonstwas heißt. Die Huber AG will nur Herrn Schulze in dessen Funktion als Vertriebsmitarbeiter der Maier GmbH adressieren und dann gebietet es die Höflich- und Menschlichkeit, dass man Herrn Schulze nicht wie einen

„namenlosen Vertriebs-Roboter“ behandelt, sondern als netten Menschen persönlich anspricht. Darüber hinaus aber ist die Huber AG nicht an Herrn Schulze interessiert. Wenn dieser das Unternehmen verlässt, hat sein Name für die Huber AG keine Bedeutung mehr; sein Nachfolger nimmt seinen Platz ein. Datenschutzrechtlich ausgedrückt ist der Zweck der Übermittlung der Daten des Repräsentanten ausschließlich die Aufnahme bzw. Fortführung des Kontakts mit dem („Absender“-) Unternehmen, das durch den Betroffenen repräsentiert wird.

Die Datenschutzbehörden, aber dies nur am Rande, unterscheiden bislang bei der Frage des Direktmarketings nicht danach, ob die Ansprache durch ein Unternehmen den Betroffenen als Privatperson (B2C) oder in seiner Eigenschaft als Unternehmensrepräsentant (B2B) betrifft. Die in verschiedenen der hier behandelten Fälle in Bezug genommene „Orientierungshilfe“ der Datenschutzkonferenz zum Thema Direktwerbung vom November 2018 unterscheidet gerade nicht zwischen der unterschiedlichen Betroffenheit der verschiedenen Zielgruppen. Aus diesem Blickwinkel könnte diese Frage demnach nur im Rahmen der Interessenabwägung einfließen, die sich aber wiederum am Wettbewerbsrecht orientieren soll (s. unten Fall 29).

Der vorliegende Fall soll aufzeigen, dass auch bei der Unterscheidung, ob eine geschäftliche oder private Ansprache eines Betroffenen erfolgt, die Realität komplexer ist. Dabei ist zunächst der sich entwickelnde Doppelcharakter eines halb geschäftlichen, halb privaten Verhältnisses datenschutzrechtlich ein Thema. Die entsprechende Verarbeitung der (auch privaten) Kontaktdaten von Herrn Schulze durch Herrn Müller ist nicht von der „Haushaltsausnahme“ (s. o. Fall 18) abgedeckt, weil die Daten zu einem doppelten Zweck genutzt werden. Soweit also Herr Schulze im Laufe der Zeit auch private personenbezogene Daten preisgegeben hat (private Anschrift, Telefonnummer, Familienverhältnisse etc.), wird man vermutlich jeweils mit einer „stillschweigenden Einwilligung“ argumentieren (s. o. Fall 8). Interessant ist dann in der Folge die Frage, wer Verantwortlicher dieser zusätzlich erhobenen Daten ist – Herr Müller privat (als die Daten „halb-privat“ Nutzender) oder die Huber AG? Oder sind beide gemeinsam Verantwortliche (s. oben Fall 16)? Muss Herr Müller nun ein Verarbeitungsverzeichnis führen (s. oben Fall 18)? Wer erteilt die Pflichthinweise, wenn Herr Schulze seine private Telefonnummer preisgibt, bzw. wer haftet, wenn diese Hinweise nicht erteilt werden? Ob man den „Datensatz“ der Kontaktdaten von Herrn Schulze in einen „Huber-AG-Teildatensatz“ (mit beruflichen Kontaktdaten, die übermittelt wurden) und einen „Müller-Teildatensatz“ (mit privaten Kontaktdaten, die erhoben wurden) aufteilen kann – also zwei gesonderte Verantwortliche jeweils für einen Teil der Daten –, ist ungewiss.

Hinzu kommt aber, dass sich auch das Interesse der Huber AG selbst an den beruflichen Kontaktdaten von Herrn Schulze verschiebt. Während es aus der Perspektive der Huber AG ursprünglich gleichgültig war, wer Vertriebsmitarbeiter bzw. Ansprechpartner der Maier GmbH ist, hat sich das Interesse – auch der Huber AG selbst, vertreten durch Herrn Müller – auf Herrn Schulze persönlich verlagert. Dieser wurde bei seinem Wechsel als natürliche Person „verfolgt" und bei seinem neuen Arbeitgeber – wiederum als Repräsentant dieses neuen Arbeitgebers – angesprochen (Direktmarketing).

Stellt dies eine Zweckänderung im Hinblick auf die Kontaktdaten von Herrn Schulze dar, wenn man den oben charakterisierten ursprünglichen Zweck zugrunde legt, der in der Aufnahme bzw. Fortführung des Kontakts mit der Maier GmbH bestand? Müsste dann die Huber AG Herrn Schulze (persönlich) zu einem schwierig zu bestimmenden „Umwidmungszeitpunkt" eine Zweckänderungsmitteilung zukommen lassen? Selbst wenn die Daten ursprünglich nicht „erhoben", sondern „nur übermittelt" worden waren (s. oben Fall 1), könnte sich diese Pflicht aus Art. 14 Abs. 4 DSGVO ergeben. Diese Regelung spricht nämlich – begrifflich weiter – von den „erlangten" Daten, anders als die Mitteilungspflicht in Art. 14 Abs. 1 bis 3 DSGVO, der sich „nur" auf die (nicht bei der betroffenen Person) „erhobenen" Daten bezieht.

Oder spricht dieser Verlauf doch dagegen, ursprünglich nur von einer „Übermittlung" der Kontaktdaten durch die Maier GmbH auszugehen, die kein „Erheben" auf Empfängerseite darstellt (s. oben Fall 1)? Möglicherweise könnte man sagen, dass die (möglichen) Zwecke bei der – dann doch anzunehmenden – „Erhebung" (auf Empfängerseite), sprich: ein „Direktmarketing" (auch) gegenüber der Person Schulze, schon von Anfang an weiter gingen als die Zwecke der Übermittlung (auf der Seite des Übermittelnden), sprich: die Aufnahme bzw. Fortführung des Kontakts (nur) mit der Maier GmbH (zufälligerweise repräsentiert durch Herrn Schulze). Diese weitergehenden Zwecke hätten sich dann nur erst später – beim Ausscheiden von Herrn Schulze – manifestiert. Dann hätten Pflichthinweise nach Art. 13 DSGVO gegenüber Herrn Schulze (persönlich) – Zweck „Direktmarketing gegenüber dem Betroffenen" – bereits bei Übergabe der Visitenkarte erteilt werden müssen. Als datenschutzrechtliche Legitimationsgrundlage für die Verarbeitung der Kontaktdaten von Herrn Schulze wäre entweder eine „stillschweigende Einwilligung" von Herrn Schulze – die aber entsprechende Informiertheit voraussetzt – oder eine Interessenabwägung (Art. 6 Abs. 1 S. 1 lit. f) DSGVO) in Betracht gekommen (s. oben Fall 8). Konnte Herr Schulze aber überhaupt in die Verarbeitung zum „erweiterten" Zweck einwilligen oder ging er davon aus, dass sich das Interesse (seinerzeit) nicht auf ihn als Person, sondern lediglich auf ihn als Repräsentant der

Maier GmbH richtete? Wäre dann also bei der späteren Manifestation eines schon von Anfang an angelegten, aber erst später – bei Weggang von Herrn Schulze – „aktivierten" weitergehenden Zwecks eine Zweckänderungsmitteilung – dann allerdings nach Art. 13 Abs. 3 DSGVO – an Herrn Schulze abzusetzen gewesen?

Die korrekte Behandlung – insbesondere auch schon das „Aufspüren" – derartiger Fälle in einem Datenschutz-Compliance-Management-System eines Unternehmens kann wohl vorsichtig als „Herausforderung" bezeichnet werden. Wenn etwas „schiefgeht", z. B. sich Herr Schulze, weil er sich über die erneute Ansprache bei der Lehmann KG ärgert, bei einer Aufsichtsbehörde über das Verhalten der Huber AG beschwert, fällt es hingegen leicht zu sagen, dass die Huber AG „ihren Laden im Griff hätte haben müssen", sprich solche Fälle hätte intern ausreichend regeln und überwachen müssen.

Fall 21:
Erlaubt das Datenschutzrecht das ewige Speichern personenbezogener Daten?

Praktischer Fall: Herr Huber, Einzelkaufmann, und die Maier OHG, deren Gesellschafter die Brüder Maier sind, haben 1982 einen Rahmenvertrag abgeschlossen. Bis 1996 hat Herr Huber unter diesem Rahmenvertrag Leistungen der Maier OHG bezogen, dann aber aus Verärgerung keine weiteren Bestellungen mehr aufgegeben. 1999 und 2012 hatte jeweils weiterer Kontakt stattgefunden, in dessen Rahmen man sich nicht über die Konditionen für weitere Lieferungen einigen konnte. Seitdem liegt das Verhältnis brach.

Alternativ: Frau Müller ist seit über 30 Jahren Rechtsanwältin und betreut laufend mehrere hundert kleinere Gerichtsverfahren im Arbeits- und Familienrecht. Zwar vernichtet sie ihre Handakten nach Ablauf der gesetzlichen Aufbewahrungsfristen, führt aber seit Beginn ihrer Anwaltstätigkeit ein stets fortgeschriebenes Verzeichnis, in dem sie Name und Kontaktdaten ihres Mandanten und des Gegners sowie eine kurze Beschreibung des Streitgegenstandes festhält.

Ein einfacher Grundgedanke der DSGVO lautet, dass personenbezogene Daten zu löschen sind, wenn der zugrunde liegende Zweck fortfällt bzw. erreicht wird, wobei gesetzliche Aufbewahrungspflichten gleichwohl zu beachten sind (bzw. als gesetzliche Legitimationsgrundlage für die weitere Speicherung die ursprüngliche Legitimationsgrundlage „ablösen"). Als Paradebeispiele für gesetzlich angeordnete Aufbewahrungsfristen werden steuerliche Aufbewahrungspflichten (§ 147 Abgabenordnung) und die Verpflichtungen zur Aufbewahrung von Handakten (z. B. §§ 50 Bundesrechtsanwaltsordnung, 51b Wirtschaftsprüferordnung, 66 Steuerberatergesetz) genannt. Im Einzelnen ist dieser Grundgedanke natürlich komplizierter (s. etwa oben Fall 14 und unten Fall 33).

➢ Die Zweckbindung während der Aufbewahrungsfrist

Dabei wird in der Praxis häufig der Grundsatz der Zweckbindung verkannt, nämlich dass, wenn der „ursprüngliche" Zweck entfällt und die Daten nur noch wegen fortbestehender Aufbewahrungspflichten gespeichert werden, sich der (Speicherungs-) Zweck auch nur noch auf die Aufbewahrung beschränkt. Man darf also nicht etwa mit den Daten tun, was man will, weil man sie ja nun „datenschutzrechtlich legal besitzt" (s. dazu im Detail oben Fall 14). In Befolgung steuerlicher Aufbewahrungspflichten aufbewahrte Dokumente dienen ei-

gentlich nur noch einer späteren Betriebsprüfung, d. h. dem Betriebsprüfer selbst und denjenigen befassten Mitarbeitern des Unternehmens, die ein „need to know" in Bezug auf die Betriebsprüfung haben. In der juristischen Literatur wird hierzu vorgeschlagen, dass in einem Archiv, d. h. nach dem Ende des ursprünglichen Erhebungszwecks, „grundsätzlich kein Zugriffsrecht bestehen" sollte. Zugriffsberechtigungen sollten dann nur nach Einzelfallprüfung und dokumentiert erfolgen.

Eine die gesetzlichen Aufbewahrungspflichten sogar noch überschreitende Speicherdauer kann – wenn nicht gerade ein Rechtsstreit anhängig ist – sicher nur über eine entsprechende Einwilligung des Betroffenen gerechtfertigt werden, die zumindest im Kontext vertraglicher Verhältnisse gesondert wählbar sein muss (Art. 7 Abs. 4 DSGVO) und nicht voreingestellt sein darf (Art. 25 Abs. 2 DSGVO). Wer rechtliche Risiken in Kauf nehmen möchte, kann längere satzungsgemäße oder vertragliche Aufbewahrungspflichten vereinbaren, die nach § 35 Abs. 3 BDSG das Löschen (weiter) verzögern können, dessen Europarechtswidrigkeit aber behauptet wird (s. auch unten Fall 33).

- Pflichtinformationen über Aufbewahrungsfristen

Über die Aufbewahrung in Erfüllung (gesetzlicher) Aufbewahrungspflichten muss auch deutlich in den Pflichthinweisen bei Erhebung aufgeklärt werden, wie die Empfehlungen des Europäischen Datenschutzausschusses vom April 2019 konkretisieren:

„In practice, if controllers see a general need to keep records for legal purposes, they need to identify a legal basis at the outset of processing, and they need to communicate clearly from the start for how long they plan to retain records for these legal purposes after the termination of a contract."

Zumindest muss hiernach die Fristlänge in Jahren angegeben werden:

„Furthermore, the controller informs data subjects that it has a legal obligation in national law to retain certain personal data for accounting purposes for a specified number of years. The appropriate legal basis is Article 6(1)(c), and retention will take place even if the contract is terminated."

➢ Das Argument der „Revisionssicherheit“ einer Archivierung

Bevor wir zum Ausgangsfall kommen, soll hier kurz auf einen – im Grunde selbstverständlichen – Bußgeldbescheid der Berliner Beauftragten für Datenschutz vom Oktober 2019 eingegangen werden. Dieser Bußgeldbescheid hat deshalb für Aufregung gesorgt, weil die Höhe des Bußgelds (EUR 14,5 Mio.) für deutsche Verhältnisse bis dahin unerreicht war. Die Deutsche Wohnen SE – ein umsatzstarkes Unternehmen, was zu einem vergleichsweise hohen Bußgeld führt – hatte, wie so viele Unternehmen in Deutschland, kein Löschkonzept für die von ihr verarbeiteten personenbezogenen Daten. Sie begründete dies damit, dass ihre Archivsoftware keine Daten löschen könne. Das ist nicht abwegig: Viele Hersteller von Dokumentenmanagementsystemen haben viele Jahre hindurch damit geworben, dass eine Archivlösung nur „revisionssicher“ sei, wenn sie keine Löschung von Daten ermöglicht. Man könnte dies böswillig auch so interpretieren, dass man sich viel Programmieraufwand für ausgefeilte Löschkonzepte sparen wollte.

Jedenfalls gibt es keine „Revisionssicherheit“ – insbesondere für steuerrelevante Daten – in dem Sinne, dass Daten nur dann „revisionssicher“ gespeichert werden, wenn sie unlöschbar „für die Ewigkeit“ konserviert werden. Weder die Abgabenordnung noch die – „nur“ ein Rundschreiben des Bundesfinanzministeriums darstellenden und damit „weit“ unter EU-Recht wie der DSGVO rangierenden – „Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“ (GoBD) verlangen eine Ewig-Archivierung. Im Gegenteil: Sämtliche maßgeblichen Textstellen verlangen, dass die Daten *„während der Dauer der Aufbewahrungsfrist“* revisionssicher (= unveränderlich) gespeichert werden müssen.

Es ist also selbstverständlich, dass nach dem Ende der maßgeblichen Aufbewahrungsfristen bzw. Aufbewahrungspflichten, gleich nach welchem Recht (wie Steuerrecht, Arbeitsrecht, Sozialversicherungsrecht etc.), personenbezogene Daten gelöscht werden dürfen und – nach Datenschutzrecht – müssen, soweit keine datenschutzrechtliche Legitimationsgrundlage für das weitere Speichern dieser Daten besteht. Man kann den im Betrieb eines „falschen“ Archivsystems liegenden „strukturellen Verstoß“ gegen die DSGVO, der dann viele Einzelverstöße in Bezug auf die jeweils datenschutzwidrig nicht gelöschten Datensätze im Einzelnen zur Folge hat, auch – wie die Berliner Datenschutzbeauftragte – auf eine Verletzung der „privacy by design“-Anforderungen (Art. 25 Abs. 1 DSGVO) stützen. Es macht dabei aus der Perspektive des Verantwortlichen keinen Unterschied, ob man die „falsche“ Software nutzt oder eine „richtige“ Software, welche die Umsetzung eines Löschkonzepts ermöglichen würde, „falsch“ – nämlich ohne ein solches Löschkonzept – nutzt.

Als betroffenes Unternehmen kann man nun in solchen Fällen nicht nur in Richtung Vorstands- bzw. Geschäftsführerhaftung denken (Compliance- bzw. Legalitätspflicht), sondern auch in Richtung einer (Mängelgewährleistungs-)Haftung des Softwarelieferanten, wenn dieser eine „rechtssichere" (oder gar „DSGVO-konforme") Software versprochen hat und dennoch keine Möglichkeit zur Löschung von Daten bietet.

➢ Wann entfällt die Legitimationsgrundlage?

Doch nun zum Ausgangsfall betreffend die Maier OHG. Die Frage, ob und wann genau eine Löschpflicht nach Art. 17 DSGVO vorliegt, wird noch unten in Fall 28 erörtert. Im vorliegenden Fall stellt sich die (Vor-)Frage, wann eine grundsätzlich (anfänglich) gegebene datenschutzrechtliche Legitimationsgrundlage „abbricht" bzw. „zu schwach wird". Im Gegensatz zum parallelen Problem bei der Interessenabwägung (s. oben Fall 8) geht es hier um die Legitimationsgrundlage Vertrag (Art. 6 Abs. 1 S. 1 lit. b DSGVO).

Situationen im vertraglichen Kontext, in denen der ursprüngliche Zweck und die ursprüngliche datenschutzrechtliche Legitimationsgrundlage nicht deutlich zu einem bestimmten Zeitpunkt entfallen, können – wie im Fall oben – darauf zurückzuführen sein, dass die Parteien in einer laufenden (handelsrechtlichen) Geschäftsbeziehung stehen, die nie förmlich beendet wurde und die „immer mal wieder" zu Folgekontakten führt, gleich, ob diese zu konkreten Einzelverträgen führen oder nicht. In der Praxis kommen diese Fälle sehr häufig vor und stellen das Datenschutzrecht auch insoweit auf die Probe, als es „eigentlich" nicht um Beziehungen zu natürlichen Personen, sondern um Beziehungen zwischen Unternehmen geht, in die „naturgemäß" natürliche Personen involviert sind (s. dazu oben Fall 20). Das Vorhalten der Daten von Herrn Huber bei der Maier OHG (und umgekehrt) könnte daher auf Art. 6 Abs. 1 S. 1 lit. b) DSGVO aufsetzen, insbesondere auch, da es in der Vergangenheit bereits Einzelverträge gegeben hat, es sich also nicht um eine reine „Marketingbeziehung" handelt.

In Bezug auf die Legitimationsgrundlage Vertrag sprechen die bisherigen juristischen Kommentatoren einerseits allgemein von einem „rechtsgeschäftlichen Verhältnis", das gegeben sein muss. Das kann man bei einer laufenden Geschäftsbeziehung – das Handelsgesetzbuch nennt das „Geschäftsverbindung" (§ 362 HGB) – durchaus annehmen. Andererseits wird aber auch ein „konkreter Vertrag, z. B. Kauf, Tausch, Miete, Schenkung" gefordert – also ein konkreter Liefervertrag, der hier schon lange nicht mehr vorlag. Dabei wird durchaus anerkannt, dass in Randbereichen von Verträgen (Treu und Glauben, Rücksichtnahmepflichten etc.) die Grenzen zur Interessenabwägung fließend seien – dies dürfte dann auch für die

„Geschäftsverbindung“ gelten. Es gibt also keine klare Grenze zwischen diesen Legitimationsgrundlagen. Wie lange also dürfen die Daten des „Geschäftspartners“ nun gespeichert werden, bis sie gelöscht werden müssen? Wie lange besteht eine „Geschäftsverbindung“ oder ein Rahmenvertragsverhältnis, wenn dieses grundsätzlich – nach Art. 6 Abs. 1 S. 1 lit. b) DSGVO oder nach Art. 6 Abs. 1 S. 1 lit f) DSGVO – eine datenschutzrechtliche Legitimationsgrundlage für die Speicherung von Kontaktdaten darstellt, aber irgendwann „verblasst“? Nur in den seltensten Fällen werden solche Beziehungen förmlich abgekündigt, meist laufen sie „irgendwann“ stillschweigend aus, wenn sie nicht mehr aktiv betrieben werden. Dennoch ist es datenschutzrechtlich ab einem – nicht genau bestimmbaren – Zeitpunkt rechtswidrig, die Daten nicht „rechtzeitig“ gelöscht zu haben.

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat in ihrem Jahresbericht 2018 diese Frage in Bezug auf B2C-Kundenverhältnisse, in denen sich die „Geschäftsbeziehung“ häufig durch die Existenz eines „Kundenkontos“ manifestiert, wie folgt beantwortet:

„Daten dürfen grundsätzlich nur so lange gespeichert werden, wie dies für die ursprünglichen Zwecke erforderlich ist. Bei einem Kundenkonto kommt es letztlich darauf an, ob dieses regelmäßig genutzt wird. Eine unbegrenzte Speicherung ist nicht zulässig. Die Unternehmen müssen Konzepte erstellen, nach welcher Zeit der Inaktivität Kundenkonten gelöscht werden, und diese durch Löschroutinen technisch-organisatorisch implementieren. Dabei kommt es auch darauf an, um welche Dienstleistung es sich handelt und in welchen Zyklen Kundinnen und Kunden typischerweise wieder bestellen. Eine Speicherung von Kundenkonten über einen Zeitraum zweijähriger Inaktivität wird allerdings regelmäßig nicht erforderlich sein.“

➢ Besondere Prüfpflichten bei der Auftragsannahme

Das Problem der „ungewissen Dauer der Verarbeitungsberechtigung“ kann auch anhand einer zweiten Situation veranschaulicht werden, die den Rechtsanwalt und dessen Möglichkeit, Kollisionsprüfungen durchführen zu können, betrifft. Ein Rechtsanwalt muss sicherstellen, dass er keine gegensätzlichen Interessen gegeneinander vertritt (§ 43a Abs. 4 BRAO). Diese gesetzliche Verpflichtung besteht zeitlich unbegrenzt, auch wenn die Pflicht zur Aktenaufbewahrung sechs Jahre nach dem Ende des Kalenderjahres der „Beendigung des Auftrags“ (wann immer das im Einzelfall ist) erlischt. Der Rechtsanwalt kann sich also datenschutzrechtlich auf eine fortbestehende *„rechtliche Verpflichtung, die die Verarbeitung nach dem Recht [...] der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert“*, berufen (Art. 17 Abs. 3 lit. b) DSGVO). Doch soll dies – auch wenn die DSGVO das nicht ausdrücklich sagt – nicht für jede beliebige gesetzliche Pflicht gelten, sondern nur für die gesetzlichen

Pflichten, die auch eine taugliche datenschutzrechtliche Legitimationsgrundlage abgeben (Art. 6 Abs. 1 S. 1 lit. c) DSGVO)? Diesbezüglich geben Art. 6 Abs. 2 und Abs. 3 DSGVO den Mitgliedstaaten auf, solche rechtlichen Verpflichtungen spezifisch mit datenschutzrechtlichen Zwecküberlegungen zu verknüpfen, von denen bei der entsprechenden Berufspflicht des Rechtsanwalts zur Kollisionsprüfung leider weit und breit nichts zu sehen ist. Im Gegenteil: Der Gesetzgeber hat sich 2017 bei der Überarbeitung der anwaltlichen Pflicht zur Aktenaufbewahrung (§ 50 BRAO) – auch im Lichte der nahenden DSGVO – nur (ausführliche) Gedanken über die datenschutzrechtliche Pflicht zur Löschung nach Ablauf der Aufbewahrungspflicht gemacht, nicht aber über die zeitlich unbegrenzte anwaltliche Kollisionsprüfungspflicht. Aber natürlich gibt es wie immer ein Hintertürchen, man beachte den letzten Satz dieser Passage der Gesetzesbegründung:

"Mit dem neuen Satz 2 wird erstmals eine Aufbewahrungsfrist für diejenigen Teile der Handakte festgelegt, die nicht unter [...] fallen. Eine solche Fristbestimmung erscheint erforderlich, um klarzustellen, für welche Dauer Handakten zur Verfügung stehen müssen. Ein datenschutzrechtlicher Löschungsanspruch der Mandantschaft ist während dieser Zeit ausgeschlossen. Der Fristbestimmung kommt dabei die wichtige Funktion zu, für alle Beteiligten auch im Hinblick auf die datenschutzrechtliche Vorgabe, dass personenbezogene Daten jeweils nur so lange gespeichert werden dürfen, wie ihre Speicherung erforderlich ist, allgemein und rechtssicher zu bestimmen, für welche Frist eine Aufbewahrung der Handakte zulässig ist. [...] – Hinweis auf die kommende DSGVO] Gerade im Hinblick auf die dort [d. h. in der DSGVO] sehr allgemeinen Regelungen zu Löschungspflichten erscheint es sinnvoll und erforderlich, dass nicht jeder einzelne Rechtsanwalt im Hinblick auf den Gegenstand jeder einzelnen Handakte gegenüber der Datenschutzaufsichtsbehörde begründen muss, warum die Aufbewahrung dieser Handakte zum Zweck der Aufsicht noch erforderlich ist, sondern für einen bestimmten Zeitraum für alle Beteiligten die Erforderlichkeit und Zulässigkeit der Aufbewahrung zu diesem Zweck gesetzlich klargestellt ist. Anschließend sind die Handakten, da sie wohl immer personenbezogene Daten enthalten werden, aufgrund der datenschutzrechtlichen Vorgaben zu vernichten, soweit sich nicht aus anderen Gründen eine Pflicht oder Befugnis zu ihrer weiteren Aufbewahrung ergibt."

Darf der Rechtsanwalt also zeitlich unbegrenzt diejenigen personenbezogene Daten speichern (Mandant, Gegner, Gegenstand), die er für spätere Kollisionsprüfungen benötigt?

Fall 22:
Mitteilung an alle: Mitarbeiter ausgeschieden!

Praktischer Fall: Herr Müller ist bei der Huber AG ausgeschieden. Er möchte mit der Huber AG nichts mehr zu tun haben und auch nicht mehr an seine Tätigkeit dort erinnert werden. Die Huber AG verfügt über verschiedene in- und ausländische Tochtergesellschaften, denen sie ihr Mitarbeiterverzeichnis jeweils konzernintern zur Verfügung stellt, damit Dritten gegenüber z. B. der zuständige Einkäufer der Huber AG benannt werden kann. Herr Müller verlangt nach seinem Ausscheiden von der Huber AG, dass sämtliche personenbezogenen Daten über ihn gelöscht werden.

In diesem Fall geht es nicht um die Frage, wann der „Löschzeitpunkt" eintritt, d. h. bis wann der Arbeitgeber die (unternehmensbezogenen Kontakt-)Daten des Beschäftigten überhaupt weiter verarbeiten (speichern) darf. Um diesen Zeitpunkt geht es unten in Fall 33. Hier wird davon ausgegangen, dass eine Löschpflicht besteht (s. dazu auch unten Fall 28).

Wenn ein Unternehmen für sich einen unternehmensinternen Löschprozess definiert, bedeutet zunächst einmal das „Löschen" von Daten, dass alles „gelöscht" wird (vgl. unten Fall 28; zur Anonymisierung als möglichem Ersatz für das Löschen s. unten Fall 32). Die dänische Datenschutzbehörde hat dies, ebenso wie die mit der Löschung verbundenen Nachweispflichten, in einer Entscheidung vom März 2019 wie folgt formuliert:

„The Agency emphasizes in its criticism that the company must be able to demonstrate by extensive means beyond a manually updated deletion log, how and when personal data is deleted in systems and backup recovery files. A retention and deletion procedure must therefore cater for deletion logs in systems and processes for ensuring that deletion is carried out based on logs in accordance with requirements as set out in internal procedures. The Agency refers in this regard to the requirement set out in article 5(2), cf. 5(1)(e), from which is follows that the data controller must be able to demonstrate that it is not possible to identify the data subject beyond what is necessary in accordance with the purposes for which the personal data is processed. The company must therefore ensure effective deletion, including in backup recovery files, and be able to demonstrate that appropriate actions are carried out to ensure this."

➢ Wie wird eine Löschung nachgewiesen?

Dies wirft gleich zu Beginn die Frage auf, wie nun ein Verantwortlicher konkret nachweist, dass er etwas gelöscht hat. Wenn jede Löschung dokumentiert wird, würde dies dem Löschzweck zuwiderlaufen – die Daten wären „immer noch da", nämlich als Teil des Löschprotokolls. Diesen Widerspruch löst auch die insoweit nur scheinbar aussagekräftige Aussage der dänischen Aufsichtsbehörde nicht vollständig. Diese legt ihr Hauptaugenmerk auf einen effektiven und dokumentierten unternehmensinternen (Lösch-)Prozess, der die notwendigen Systeme und Kontrollen (gleichbedeutend mit Regelungen und Vorkehrungen oder mit organisatorischen und technischen Maßnahmen) etabliert und neben der Prozessdokumentation (Verfahrensbeschreibung) auch zu entsprechender, automatisiert erstellter Kontrolldokumentation (Löschprotokoll) führt. Dies lässt aber offen, inwieweit die einzelnen gelöschten Daten (bzw. Metadaten) dem Löschprotokoll entnehmbar sein müssen.

Man kann dies auch pragmatischer sehen. Die FAQ-Sektion des Bayerischen Landesamts für Datenschutzaufsicht gibt in Bezug auf die Betroffenenrechte insgesamt auf die Frage *„Bin ich verpflichtet, zu speichern, dass ich auf Antrag Auskunft erteilt, Daten gelöscht oder berichtigt habe?"* eine gewohnt lakonische Antwort:

„Nein. Zur Erfüllung der Rechenschaftspflicht reicht es aus, dass ich einen entsprechenden Prozess zur Bearbeitung von Betroffenenrechten nachweisen kann."

Auch dies lässt aber offen, ob die Existenz einer Prozessdokumentation ausreicht oder der Prozess zum Beweis seiner „Wirksamkeit" nicht auch (irgend)eine Kontrolldokumentation über durchgeführte Löschvorgänge produzieren muss. Eine Möglichkeit, die insoweit auf technischer Ebene diskutiert wird, ist, im Rahmen eines Löschprotokolls die Hash-Werte der gelöschten Datenobjektive zu speichern (s. zum Begriff der Hash-Werte auch unten Fall 32), sodass später zwar anhand der Originaldaten (wenn diese „von außen" an das Unternehmen herangetragen werden) nachvollzogen werden kann, dass die entsprechenden Daten seinerzeit (im Rahmen des Löschprozesses) gelöscht wurden. Aus dem Hash-Wert kann aber das gelöschte Datum selbst nicht mehr ermittelt werden. Das funktioniert technisch aber nur bei exakt gleichem „Input" der Hash-Funktion; schon die kleinste Abweichung z. B. bei der Schreibweise eines Namens (oder die Hinzufügung eines Leerzeichens) führt dann zu einem abweichenden Hash-Wert und letztlich dazu, dass der Nachweis des damaligen Löschens unklar bleibt.

Unabhängig davon bedeutet Löschen aber auch, dass, wenn dieselben Daten (ggf. aus anderen Quellen) später wieder erhoben oder „importiert" werden, sich der Verantwortliche

nicht an die frühere Verarbeitung „erinnern“ kann. Will also der Betroffene ausschließen, dass seine Daten auch in Zukunft aufgrund eines „Neuimports“ verarbeitet werden, muss er dem Verantwortlichen eigentlich die (zeitlich unbeschränkte) Einwilligung erteilen, seine Identität in einer „Blacklist“ beim Verantwortlichen zu speichern. Dies ist in der Praxis insbesondere bei Direktmarketing (Werbung) gegenüber dem Betroffenen der Fall.

- Die Liste der Empfänger

Der Löschprozess als solcher muss während seiner Ausführung auf bestimmte Metadaten zurückgreifen können, die während des Lebenszyklus‘ der personenbezogenen Daten anfallen und entsprechend laufend zu dokumentieren sind. Gemeint sind hier insbesondere – für die Zeit zwischen Erhebung und Löschung – die *„Empfänger, denen personenbezogene Daten offengelegt wurden“* (Art. 19 DSGVO). Denn einerseits ist diesen Empfängern die Löschung mitzuteilen, andererseits sind der betroffenen Person bei einem etwaigen Auskunftsersuchen (Art. 17 DSGVO) die Empfänger mitzuteilen. Dasselbe gilt im Übrigen auch für die Berichtigung, z. B. im Falle einer Adressänderung, sowie für die Einschränkung der Verarbeitung, z. B. bei einem Widerspruch des Betroffenen im Falle einer Interessenabwägung. Nur am Rande: Die Verpflichtung, dem Betroffenen sämtliche Empfänger mitzuteilen, kann für die Lösung der Frage eine Rolle spielen, ob ein Übermittelt-Erhalten eine „Erhebung“ darstellt, welche ihrerseits Pflichthinweise durch den Empfänger auslöst (s. oben Fall 1). Wäre nämlich jeder Empfänger einer Übermittlung verpflichtet, dem Betroffenen den Empfang mitzuteilen (Art. 14 DSGVO), dann wäre die Verpflichtung des übermittelnden Verantwortlichen, dem Betroffenen auf dessen Anforderung hin die (Historie der) Übermittlungsempfänger mitzuteilen, redundant. Wie auch immer: Sowohl die Mitteilung der Löschung an die Empfänger als auch die Mitteilung der Empfänger an den Betroffenen setzt zunächst einmal voraus, dass über die Empfänger genau „Buch geführt“ wird, und zwar ausnahmslos.

- Übermittlung und Haftung

Vor diesem Hintergrund stellen sich in der Praxis insbesondere zwei Folgefragen. Einerseits ist offen, was die Huber AG genau bei Weitergabe der Daten beachten musste. Im Fallbeispiel können die Tochtergesellschaften – je nach Ausgestaltung des gemeinsamen Mitarbeiterverzeichnisses – entweder eigenständige Verantwortliche sein, denen die Kontaktdaten von der Huber AG „übermittelt“ wurden, oder sie sind aufgrund eines „gemeinsam geführten Mitarbeiterverzeichnisses“ gemeinsam Verantwortliche (s. o. Fall 16). In beiden Fällen hat

die jeweilige Tochtergesellschaft, wenn sie von einem Löschungsverlangen eines Betroffenen erfährt (durch die Huber AG oder anderweitig) – und eigentlich nicht nur dann, sondern immer –, zu prüfen, ob sie einer Löschungspflicht unterliegt.

Aber auch unabhängig von dieser gesetzlichen Verpflichtung könnte es im Interesse der Huber AG gelegen haben, mit allen zumutbaren Mitteln sicherzustellen, dass ein Löschungsverlangen eines Betroffenen gegenüber der Huber AG auch von ihren Tochtergesellschaften (oder sonstigen dritten Empfängern der Daten des Betroffenen) umgesetzt wird. Denn schon wegen der EU-rechtlichen „Konzern-Sippenhaftung", die im EU-Kartellrecht entwickelt wurde, kann die Huber AG für Datenschutzverstöße ihrer Tochtergesellschaften verantwortlich sein. Doch selbst ohne Rückgriff auf solche Einstandspflichten für Tochtergesellschaften könnte sie für eine vom Empfänger der Daten unterlassene Löschung verantwortlich gemacht werden. Das steht zwar nirgends so klar in der DSGVO, wird aber von Kommentatoren sinngemäß im Zusammenhang mit der (gesamtschuldnerischen) Haftung postuliert (s. o. Fall 12): Jeder Verantwortliche in einer „Datenkette" haftet für den Gesamtschaden des Betroffenen, wenn er „auf irgendeine Art und Weise für den entstandenen Schaden verantwortlich ist" oder sogar nur an der Verarbeitung irgendwie beteiligt war. Die Huber AG ist im Umkehrschluss nur dann nicht verantwortlich für ein datenschutzwidrig unterlassenes Löschen beim Empfänger, „wenn sie nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist" (Art. 82 Abs. 3 DSGVO). Der Gesetzgeber wollte den Betroffenen nicht zumuten, sich „die Kette entlangzuhangeln": Am Ende soll jeder haften, der irgendwie „die Finger im Spiel hatte".

Wenn das nun bedeuten würde, dass sich jeder beteiligte Verantwortliche im eigenen Interesse vertraglich absichern sollte, um „alles getan" zu haben und einer Haftung zu entgehen (Exkulpation), wie weit müssen dann die Bemühungen gehen? Sprich: Wenn ein Empfänger sich weigert, derartige (vertragliche) Regelungen zu akzeptieren, müsste dann die Übermittlung der Daten an den Dritten unterbleiben, um eine eigene Haftung wegen eines möglicherweise später „unzuverlässigen" Übermittlungsempfängers auszuschließen? Weiter soll die erste Folgefrage der Mitteilungspflichten beim Löschen hier nicht vertieft werden.

➢ Unverhältnismäßiger Aufwand?

Andererseits – als zweite Folgefrage – besteht die Verpflichtung, die Löschung bzw. Berichtigung den Empfängern mitzuteilen, nicht, wenn *„sich dies als unmöglich erweist oder mit einem unverhältnismäßigen Aufwand verbunden ist"* (Art. 19 DSGVO). Das sind natürlich wieder wachsweiche Formeln, zumal ein „gesetzesgleicher" Erwägungsgrund hier fehlt, der einen Anhaltspunkt für den konkreten gesetzgeberischen Willen aufzeigen würde. Erschwert

wird die Einhaltung dieser Verpflichtung – wie so oft – dadurch, dass den Verantwortlichen die Beweislast trifft nachzuweisen, dass Unmöglichkeit oder Unverhältnismäßigkeit vorlag. Kann er diesen Beweis nicht führen, hat er seine Pflicht zur Mitteilung verletzt. Einigkeit herrscht zwar im Prinzip darüber, dass ein unverhältnismäßiger finanzieller Aufwand zur Unverhältnismäßigkeit führen kann, aber wo hier die Grenzen liegen, ist unklar. Eine typische Situation, die jeden (Compliance-Verantwortlichen), der Haftungsrisiken durch gestaltende Maßnahmen effektiv vermeiden möchte, in den Wahnsinn treiben kann. Beispielhaft sei hier auf eine Entscheidung der polnischen Datenschutzbehörde verwiesen, die sich auf den Parallelfall des Aufwands für die Erteilung von Pflichtinformationen bezieht: Während von 679.000 Datensätzen die E-Mail-Adressen vorlagen und den Betroffenen die Pflichtinformationen per E-Mail zur Verfügung gestellt wurden, hatte man bei 5,7 Millionen weiteren Datensätzen, zu denen nur die postalische Adresse vorlag, mit Hinweis auf die Unverhältnismäßigkeit der Kosten die Mitteilung von Pflichtinformationen (nach Art. 14 Abs. 5 lit. b DSGVO) unterlassen. Die polnische Datenschutzbehörden sah demgegenüber keinen „unverhältnismäßigen Aufwand" für diese postalische Versendung.

In einem Fallbeispiel des sog. „Working Paper 260" der Artikel-29-Datenschutzgruppe, später vom Europäischen Datenschutzausschuss für die DSGVO bestätigt, über Bezugs- bzw. Kontaktpersonen (Angehörige bzw. nahestehende Dritte), die in Anmeldeformularen in Krankenhäusern angegeben werden können, klingt dies allerdings für „großvolumige Fälle" anders:

„A large metropolitan hospital requires all patients for day procedures, longer-term admissions and appointments to fill in a Patient Information Form which seeks the details of two next-of-kin (data subjects). Given the very large volume of patients passing through the hospital on a daily basis, it would involve disproportionate effort on the part of the hospital to provide all persons who have been listed as next-of-kin on forms filled in by patients each day with the information required under Article 14."

Wenn also angesichts dieser widersprüchlichen Signale die Versendung von (vielen) Briefen im Rahmen der Pflichtinformationen keinen sicher unverhältnismäßigen Aufwand darstellt, bleibt als „sicherer Hafen" im Rahmen der Mitteilungspflicht über die Löschung nur noch der Fall von „Unverhältnismäßigkeit" übrig, dass die Empfänger tatsächlich nicht mehr ermittelt werden können. Neben dem Fall der Nichtauffindbarkeit (bei Gesellschaften nach Liquidation oder Insolvenz auch: „Vollbeendigung") des Empfängers kann dies eigentlich nur bei einer Veröffentlichung der Daten einschlägig sein, sodass die Empfänger (und die Empfänger der Empfänger etc.) im Einzelnen unbekannt sind. Der Fall der Veröffentlichung

ist jedoch, was den Umfang der Pflichten bei Löschung angeht, bereits speziell geregelt (Art. 17 Abs. 2 DSGVO): Hiernach muss der Verantwortliche sinngemäß „einschlägige" dritte Multiplikatoren, die typischerweise solche Informationen „aufsaugen" und als Links zur Verfügung stellen – insbesondere also Suchmaschinenbetreiber –, vom Löschungsverlangen informieren. Am Ende bleibt also völlig unklar, auf welche Fälle der Unverhältnismäßigkeit man sich hier sonst berufen könnte.

Die vorgenannten Einschränkungen der Pflicht zur Mitteilung an die Empfänger – Unmöglichkeit oder Unverhältnismäßigkeit – gelten übrigens nicht schon für die (vorgelagerte) Verpflichtung, die Empfänger überhaupt erst einmal aufzuzeichnen. Man kann sich also nicht damit „herausreden", dass schon die Aufzeichnung der Empfänger unmöglich oder unverhältnismäßig gewesen sei, sondern nur damit, dass die Mitteilung gegenüber diesen Empfängern unmöglich oder unverhältnismäßig ist. Das Argument gegenüber dem Betroffenen, man könne ihm die Empfänger nicht mitteilen, weil diese – warum auch immer – nicht erfasst wurden („Das sieht unsere Software nicht vor"), ist daher mit Vorsicht zu genießen. In diesem Zusammenhang schließlich noch folgende Randnotiz: Die Pflicht zur Mitteilung der Empfänger bezieht sich zeitlich auf frühere Empfänger, ohne dass ein festes „Startdatum" definiert werden könnte. Nach der sog. „Rijkeboer"-Entscheidung des EuGH aus dem Jahr 2009 zur EU-Datenschutzrichtlinie gilt ein „dynamischer Maßstab" in einer Abwägung zwischen Aufwand und Nutzen. Eine Grenze geben insofern möglicherweise (allenfalls) die Aufbewahrungsfristen für die Daten – soweit es solche gibt – vor.

- Mitteilung gegenüber Dritten

Die Pflicht zur Mitteilung gegenüber den Empfängern, dass Daten zu löschen sind, gilt natürlich nicht nur gegenüber Konzernunternehmen. Letztlich sind sämtliche „Empfänger-Verantwortlichen" zu speichern, damit sie später benachrichtigt werden können. Im Falle des Ausscheidens eines Mitarbeiters aus einem Unternehmen müsste dies wahre Kaskaden an Mitteilungen lostreten.

Dabei geht es nicht nur um Namen bzw. unternehmensbezogene Kontaktdaten („Visitenkartendaten", dazu oben Fall 1), sondern auch um „Werbedaten" wie Bilder der Mitarbeiter, mit denen der Verantwortliche wirbt. Hier stellt sich schon das Problem der ursprünglichen Legitimationsgrundlage bei der Anfertigung. Im Gegensatz zu Personalaktendaten, unternehmensbezogenen Kontaktdaten und Bewegungsdaten kann § 26 BDSG nicht mehr als taugliche Legitimationsgrundlage angesehen werden, wie der Hessische Beauftragte für Datenschutz in seinem Tätigkeitsbericht 2018 ausführt:

„§ 26 Abs. 1 BDSG verlangt, dass die Datenverarbeitung zur Durchführung des Beschäftigungsverhältnisses „erforderlich" ist. Erforderlichkeit bedeutet, dass die berechtigten und schützenswerten Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht der/des Beschäftigten zu einem schonenden Ausgleich zu bringen sind, der beide Interessen möglichst weitgehend berücksichtigt. Notwendig ist somit eine Interessenabwägung zwischen den Belangen der/des Beschäftigten und der verantwortlichen Stelle im Sinne einer Verhältnismäßigkeitsprüfung. § 26 Abs. 1 Satz 1 BDSG kommt danach als Rechtsgrundlage nur für den Fall in Betracht, dass die visuelle Präsentation des/der Beschäftigten Gegenstand des Arbeitsvertrages wäre, wie zum Beispiel bei einem Fotomodell. Sollen jedoch „normale" Mitarbeiter/-innen bei der öffentlichen Darstellung des Unternehmens in Form von Bildern oder Filmsequenzen mitwirken, ist dies zur Durchführung des Beschäftigungsverhältnisses regelmäßig nicht erforderlich, da es überwiegend werblichen Zwecken dient."

Im weiteren Verlauf thematisiert der Hessische Datenschutzbeauftragte dann aber dennoch § 26 BDSG als Legitimationsgrundlage und stellt fest – was wohl auch für die gerade noch geforderte Interessenabwägung gelten muss –, dass nach dem Ende des Beschäftigungsverhältnisses die Legitimationsgrundlage entfällt (s. auch unten Fall 33 zu den Bewegungsdaten und Fall 28 zu den Voraussetzungen für das Löschen):

„Eingaben, die meiner Behörde vorliegen, betreffen bislang regelmäßig den Sachverhalt, dass eine Mitarbeiterin/ein Mitarbeiter aus dem Unternehmen ausgeschieden ist, ihr/sein Bild aber weiterhin auf der Webseite des Unternehmens veröffentlicht ist. Sofern die Veröffentlichung auf § 26 Abs. 1 Satz 1 BDSG gestützt war, fällt mit Ausscheiden des/der Beschäftigten der Zweck zur Veröffentlichung weg, mit der Folge, dass Art. 17 Abs. 1 lit. a DS-GVO greift: ‚Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.'"

Das Bayerische Landesamt für Datenschutzaufsicht geht in seiner FAQ-Sektion bei der Frage *„Dürfen Fotos von Mitarbeitern, Vereinsmitgliedern oder Dritten auf der Website veröffentlicht werden?"* nicht so detailliert auf die Details des Gesetzes und insbesondere auf die Grenzen einer Interessenabwägung und auf die Löschpflicht ein, sondern formuliert etwas „hemdsärmelig":

„Ja. Die Veröffentlichung ist in der Regel nach entsprechender Interessenabwägung auch ohne Einwilligung zulässig. Im Zweifel, insbesondere bei Kindern, Jugendlichen sowie anderen Schutzbedürftigen sollte jedoch vorab eine Einwilligung eingeholt werden. Sind die

Fotos erst einmal veröffentlicht, gibt es im Internet keine 100%ige Löschung. Außerdem sollten die abgebildeten Personen vorab über die Veröffentlichung informiert werden.“

Wurden solche „Werbedaten“ in Bildform nun gezielt einzelnen Empfängern übermittelt – etwa als Teil einer Teamkarte, sodass der Kunde sehen kann, wie die Personen aussehen, mit denen er es zu tun hat –, so müssen diese Empfänger ebenso von der notwendigen Löschung benachrichtigt werden. Hinzu kommt die „Internet-Löschpflicht“ nach Art. 17 Abs. 2 DSGVO, die „angemessene Maßnahmen“ zur Information an Multiplikatoren fordert, was – wie die bayerische Datenschutzaufsicht zu Recht anmerkt – aber nicht mit einer 100%-Erfolgsgarantie versehen ist.

➢ Wo ist die Grenze?

Betrachten wir abschließend noch ein kurzes Beispiel – natürlich weit hergeholt und damit absurd anmutend – im Zusammenhang mit einer Wursttheke in einem Supermarkt. Auf dem Bon der (digitalen) Kasse der Wursttheke, der anschließend an der Supermarktkasse gescannt wird, steht „Sie wurden bedient von Herrn Martin Huber“. Das entsprechende Etikett nimmt der Kunde mit nach Hause.

Handelt es sich um die Übermittlung personenbezogener Daten des Wurstthekenverkäufers an den Kunden oder um „aufgedrängte Daten“ (s. dazu oben Fall 1)? Normalerweise nicht, weil der Kunde zuhause gewöhnlich den Beleg wegwirft, d. h. es liegen gar keine personenbezogenen Daten im Sinne der DSGVO-Definition vor (s. dazu unten Fall 23). Heftet der Kunde die Wurstthekenbons aber schön geordnet in eine Akte ab, weil er ein (Anwesenheits-)Profil von Herrn Martin Huber erstellen möchte, so würde es sich doch um eine (analoge) strukturierte Sammlung personenbezogener Daten handeln und der Kunde wäre wohl Verantwortlicher im Sinne der DSGVO für die an ihn übermittelten (übergebenen) Daten. Dabei wird der Kunde aber wohl nicht auf eine taugliche DSGVO-Legitimationsgrundlage zurückgreifen können, auch wenn er täglich oder wöchentlich einen Bon in die Hand gedrückt bekommt. Er wäre also eigentlich, wenn er beabsichtigen würde, die Daten DSGVO-mäßig strukturiert zu „horten“, verpflichtet, die Bons sofort nach dem Einkauf zu vernichten. Macht er sich darüber keine Gedanken und behält die Bons als (unstrukturierte) „Zettelsammlung“, könnte er hingegen beliebig viele Bons horten.

Muss sich der Supermarkbetreiber schon unabhängig davon, ob der Bon in den Händen des Kunden personenbezogene Daten im Sinne der DSGVO darstellt, überlegen, ob das Aufdrucken des Verkäufernamens „erforderlich“ für die Durchführung des Beschäftigungsverhältnisses mit Herrn Martin Huber ist bzw. im Sinne der Datenminimierung unterlassen werden

sollte? Muss der Supermarktbetreiber – schließlich hat er selbst die personenbezogenen Daten von Herrn Martin Huber aktiv „herausgegeben“ – ahnen oder gar abfragen, ob der Kunde – wohl rechtswidrig – die Bons (mit dem Namen und der Tatsache der Anwesenheit von Herrn Martin Huber an einem bestimmten Tag um eine bestimmte Uhrzeit) hortet, sodass es sich um eine „Datenkette“ handelt (s. oben Fall 12)? Muss er die Daten des Kunden erheben, um ihm eine Mitteilung zukommen lassen zu können, wenn Herr Huber um Löschung seiner personenbezogenen Daten bittet bzw. aus der Supermarktbetreibergesellschaft ausscheidet? Oder ist dies wegen Art. 11 DSGVO nicht notwendig (s. unten Fall 39) oder weil der Supermarktbetreiber davon ausgehen darf, dass die Daten ohnehin sofort beim „Übermittlungsempfänger“ gelöscht werden? Der Fall ist (zu) alltäglich und mag in dieser Form in der Praxis „nie“ bei Datenschutzbehörden oder Gerichten aufschlagen, aber ihrer Struktur nach stellen sich derartige Probleme in anderem Kontext in der Praxis durchaus häufig.

Fall 23:
Datenkontakt während der Vertragsanbahnung

Praktischer Fall: Die Maier GmbH erwägt, eine Software zur Mitarbeiter-Einsatzplanung individuell programmieren zu lassen. Zu diesem Zweck lädt sie Herrn Krämer, einen Mitarbeiter des Softwareentwicklungshauses Lehmann KG, zu sich ein, damit dieser danach ein Angebot für die Softwareentwicklung erstellen kann. Während seines Besuches werden Herrn Krämer die bestehenden Systeme bzw. Datenbanken der Personalabteilung der Maier GmbH gezeigt, um Herrn Krämer die Möglichkeit zu geben, den Aufwand der gewünschten automatischen Datenübernahme aus diesen Systemen abschätzen zu können. Dabei werden spontan anhand einiger Beispiele verschiedene Datenfelder und deren Inhalt angesehen. Es handelt sich beispielsweise um Mitarbeiternamen, Krankheitsmeldungen, Leistungsbeurteilungen etc. Herr Krämer macht sich jeweils allgemeine Aufzeichnungen über die Datenstrukturen und hin und wieder fertigt er Screenshots als Erinnerungsstütze an. Beim späteren Ansehen der Screenshots stellt Herr Krämer zufällig fest, dass ein Bekannter von ihm bei der Maier GmbH tätig ist, und erfährt, dass dieser in letzter Zeit auffällig oft krank gewesen ist. Die Lehmann KG gibt ein Angebot ab, das aber von der Maier GmbH nicht angenommen wird.

Das erste, was hier „on the edge" ist, ist die Frage, ob die DSGVO überhaupt Anwendung findet. Nach Art. 2 Abs. 1 DSGVO gilt die Verordnung *„für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen"*. Man kann zunächst einmal „von unten nach oben" festhalten: Manuelle Verarbeitungsschritte – Paradebeispiel ist das Beobachten einer Person durch einen Detektiv – sind nicht Gegenstand des Datenschutzrechts (was nicht heißt, dass nicht andere Rechtsgebiete relevant sein können). Auch dann, wenn der Detektiv den von ihm (handschriftlich?) verfassten Bericht in einer „unstrukturiert geführten Akte" dem Auftraggeber zukommen lässt, liegt (wohl) kein datenschutzrechtlich relevanter Vorgang vor. Sobald es sich allerdings um ein (analoges oder digitales) „Dateisystem" handelt, in die personenbezogene Daten „hineingespeichert" werden oder werden sollen, gilt die DSGVO von Anfang an, also auch für die manuelle Verarbeitung (inklusive Erhebung). Ein Dateisystem ist nach Art. 4 Nr. 6 DSGVO eine *„strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich ist, unabhängig davon, ob sie zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird"*. Ein Paradebeispiel für ein analoges Dateisystem ist ein Karteikasten oder eine „strukturierte Akte", wie auch immer diese konkret von der „unstrukturierten Akte" abzugrenzen ist. Da ein (auch digitales) Dateisystem

(angeblich) zumindest zwei Elemente enthalten muss (sonst wäre es keine Daten-„Sammlung"), reicht ein einzelnes Dokument nicht aus; die Untergrenze wären im digitalen Bereich etwa zwei auf einem Computer gespeicherte Datensätze (wie Briefe etc.), die personenbezogene Daten enthalten.

Sind nun die Screenshots, die personenbezogene Daten in Form unstrukturierter Daten (Bilddatei) enthalten, Gegenstand der DSGVO, wenn der Dateiname jeweils „Besuch bei Maier GmbH Screenshot Nr. X" lautet? So eindeutig ist das - anders als bei Abbildungen erkennbarer Personen – nicht. Eine Bilddatei kann ein Dateisystem sein, wenn eine (automatische) Identifizierung der im Bild enthaltenen personenbezogenen Angaben möglich ist. Nun kann man heutzutage in jedem Bild Schriftzeichen einschließlich z. B. Kfz-Kennzeichen erkennen (OCR), in jedem Video Gesichter identifizieren und mit jeder Tonaufnahme kann ein Stimmabgleich durchgeführt werden. Unerheblich hingegen ist (wegen des Kriteriums der *„Sortierung bzw. Auswertbarkeit der Daten nach bestimmten Kriterien"* einer Datensammlung), dass Herr Krämer zufällig auf den Bildern personenbezogene Daten „entdeckt" hat: Die Sortierung oder Auswertung muss nicht stattgefunden haben.

Geht man davon aus, dass die DSGVO auf die beschriebene „Erhebungs"-Tätigkeit des Softwareentwicklungshauses Lehmann KG Anwendung findet, so stellt sich – neben der Standard-Thematik der Pflichthinweise – die Frage der Legitimationsgrundlage für die Verarbeitung durch die Lehmann KG (repräsentiert durch Herrn Krämer). Hier scheidet zunächst die Durchführung vorvertraglicher Maßnahmen – immerhin soll ja ein Angebot für einen künftigen Vertrag erstellt werden – aus, denn diese erfolgen nicht „auf Anfrage der betroffenen Person(en)", sprich der Beschäftigten, deren Daten hier sichtbar sind. Neben Art. 6 Abs. 1 S. 1 lit. b) DSGVO scheidet aber auch § 26 BDSG aus, denn das Abfotografieren geschieht nicht „für Zwecke des Beschäftigungsverhältnisses". Es bleibt somit nur die Interessenabwägung und die Frage, ob die Screenshots „erforderlich" sind, damit die – sicher berechtigten – Interessen der Maier GmbH nach einer Software zur Mitarbeiter-Einsatzplanung „gewahrt" werden, wie es in Art. 6 Abs. 1 S. 1 lit. f) DSGVO so schön heißt.

Was bedeutet nun dabei „erforderlich" (s. auch oben Fall 17)? Man kann das so umschreiben: Eine für die betroffene Person weniger invasive Alternative existiert entweder nicht oder ist für den Verantwortlichen nicht zumutbar. Also: Ist eine Anonymisierung der Daten bzw. die Vorbereitung von „Fake"-Datensätzen im Vorfeld der Sitzung zumutbar, d. h. die Bildschirminhalte, die man mit Herrn Krämer bespricht, werden vorab so „frisiert", dass dort keine personenbezogenen Daten ersichtlich sind (s. dazu auch unten Fall 34)? Das würde schließlich auch dem Grundsatz der Datenminimierung entsprechen (Art. 5 Abs. 1 lit. c) DSGVO),

der herkömmlich so verstanden wird, dass dann, wenn der Verarbeitungszweck mit anonymen Daten erreicht werden kann, die Verarbeitung von nicht-anonymen Daten datenschutzwidrig wäre.

Nun dürfen mal wieder die Würfel gerollt werden. Auf der einen Seite wird man sagen können, dass vor dem Besuch nicht absehbar ist, „wohin überall geklickt werden wird", und dass die Software nicht mehrere alternative Datenquellen, zwischen deren Ansicht hin- und hergeschaltet werden kann, bzw. eine automatisierte Anonymisierung unterstützt. Die Software ist also insoweit nicht „datenschutzfreundlich", was ja ebenso für die (Fern-) Wartung gelten würde, bei der ebenfalls ein Dritter (der Softwarehersteller) auf die Software zugreifen muss (s. dazu noch unten Fall 27). Auf der anderen Seite könnte man sagen, dass eine Verletzung der Pflicht, datenschutzfreundliche Software einzusetzen (Art. 25 Abs. 1 DSGVO), nicht dem Verantwortlichen (durch eine dann doch „positive" Interessenabwägung) zum Vorteil gereichen soll, und dass schließlich das Interesse der Betroffenen, dass ihre sensiblen Mitarbeiterdaten nicht an Dritte weitergegeben werden, durchaus gewichtig ist, sodass auch der zusätzliche Aufwand des Verantwortlichen, vorab irgendeine Form der „Verschleierung" der personenbezogenen Daten vorzunehmen, gerechtfertigt ist.

Wer sich fragt, ob diese Abwägung zu einem klaren und „gerechten" Ergebnis führen wird, dem sei als Trost die Lektüre des Buchs „Legitimation durch Verfahren" von Niklas Luhmann sowie die Beschäftigung mit dem für das Verfassungsrecht konzipierten „Prinzip der praktischen Konkordanz" (Konrad Hesse) empfohlen. Es geht für die hier involvierten Unternehmen (als Privatrechtssubjekte) nicht mehr nur einfach darum, ein Gesetz zu befolgen; es geht darum, dass in einem dokumentierten Verfahren *„verfassungsrechtlich geschützte Rechtsgüter in der Problemlösung einander so zugeordnet werden müssen, dass jedes von ihnen Wirklichkeit gewinnt. […] Beiden Gütern müssen Grenzen gesetzt werden, damit beide zu optimaler Wirksamkeit gelangen können"*. Gewöhnlich geschieht diese Güterabwägung durch den Gesetzgeber oder die staatliche Verwaltung, nicht aber durch Privatrechtssubjekte wie Unternehmen, Organisationen und natürliche Personen (die ja auch Verantwortliche im Sinne der DSGVO sein können). Das dahinterstehende, grundsätzliche Problem für den Rechtsanwender wird im Anhang unten noch weiter erörtert.

Fall 24:
Übermittlung an ein Drittland?

Praktischer Fall (basiert auf Fall 23): Die Maier GmbH erwägt, eine Software zur Mitarbeiter-Einsatzplanung individuell programmieren zu lassen. Zu diesem Zweck lädt sie Herrn Smirnow, einen Mitarbeiter des russischen Softwareentwicklungshauses „Russia Software OOO", zu sich ein, damit dieser danach ein Angebot für die Softwareentwicklung erstellen kann. Während seines Besuches werden Herrn Smirnow die bestehenden Systeme bzw. Datenbanken der Personalabteilung der Maier GmbH gezeigt, um Herrn Smirnow die Möglichkeit zu geben, den Aufwand der gewünschten automatischen Datenübernahme aus diesen Systemen abschätzen zu können. Dabei werden spontan anhand einiger Beispiele verschiedene Datenfelder und deren Inhalt angesehen. Es handelt sich beispielsweise um Mitarbeiternamen, Krankheitsmeldungen, Leistungsbeurteilungen etc. Herr Smirnow macht sich jeweils allgemeine Aufzeichnungen über die Datenstrukturen und hin und wieder fertigt er als Erinnerungsstütze Screenshots mit seinem Tablet-PC an, den er wieder mit nach Russland nimmt. Die Russia Software OOO gibt ein Angebot ab, das aber von der Maier GmbH nicht angenommen wird.

Wenn man unterstellt, dass es sich überhaupt um einen Anwendungsfall der DSGVO handelt (s. oben Fall 23), so würde die Aufnahme der Screenshots wohl ein „Erheben" von Daten durch die „Russia Software OOO" (repräsentiert durch Herrn Smirnow) darstellen. Im Unterschied zu Fall 23 werden diese Daten nun in ein Drittland – Russland – „exportiert", für das kein Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO) vorliegt. Für eine „Übermittlung" in ein Drittland gelten nun nach Art. 44 bis 50 DSGVO vergleichsweise strenge Anforderungen. Der Begriff der „Übermittlung" wird in der DSGVO nicht weiter definiert, sondern nur als Fall der „Offenlegung" bezeichnet (Art. 4 Nr. 2 DSGVO) und dann überwiegend in den genannten Artikeln 44 bis 50 benutzt (s. auch oben Fall 1). Nach gängigem Verständnis ist das Übermitteln in ein Drittland weit zu verstehen, „sei es durch das Weitergeben von Daten an einen Empfänger im Drittland bzw. sonstige Bereitstellung, Zugänglichkeit im bzw. Abrufbarkeit aus dem Drittland, oder sei es in Form der Speicherung auf Servern, die im Drittland belegen sind". Jedenfalls muss eine „Offenlegung im Drittland" erfolgen.

Im vorliegenden Fall erhebt die „Russia Software OOO" die Daten in der EU, nämlich vor Ort in Deutschland bei der Maier GmbH. Vorausgesetzt, hierbei werden sämtliche einschlägigen Pflichten (Pflichthinweise etc.) eingehalten und es gibt eine taugliche Legitimationsgrundlage (s. oben Fall 23), stellt dies auch gar kein Problem dar. Nun werden sie aber – in

der Sprache des Strafrechts – nicht per Datenfernübertragung in ein Drittland „übermittelt“, sondern sie werden auf einem Datenträger (Tablet-PC von Herrn Smirnow) in ein Drittland „verbracht“. Ist dieses Verbringen begrifflich im „Übermitteln“ des Art. 44 DSGVO enthalten? Sprachlich eher weniger. Allerdings sind verschiedene Juristen der Meinung, dass von Art. 44 DSGVO alle Vorgänge erfasst werden sollen, bei denen eine Drittlandsgrenze überschritten wird, also gleich in welcher Weise. Warum hat man dann aber den einengenden Begriff der Übermittlung verwendet und die DSGVO nicht gleich so abgefasst, wenn das so gemeint gewesen wäre? Um die Verwirrung zu komplettieren: In der englischen Sprachfassung der DSGVO wird an dieser Stelle nicht das dort sonst übliche Pendant für das in Art. 4 Nr. 2 DSGVO enthaltene Wort „Übermittlung“, nämlich „transmission“, sondern das sonst in der englischen Sprachfassung nicht genutzte Wort „transfer“ verwendet.

Hinzu kommt, dass im Moment der Überschreitung der EU-Außengrenze (Herr Smirnow sitzt im Flugzeug nach Russland) unklar ist, ob Herr Smirnow seine Screenshots jemals wieder ansehen wird. Vielleicht vergisst er sogar, dass er diese angefertigt hat, und greift ausschließlich auf seine sonstigen Aufzeichnungen zurück. Lässt sich nun im Moment der „Übermittlung“ – eine solche unterstellt – sagen, ob eine „Offenlegung im Drittland“ erfolgen wird?

Eine weitere Dimension derartiger Fälle wird deutlich, wenn man sich vor Augen hält, dass man nicht einmal in ein Drittland ausreisen muss (mit personenbezogenen Daten im Gepäck), um Daten – vielleicht nicht ganz bewusst – in ein Drittland zu „exportieren“. Viele Daten werden automatisch (im „Backend“) „in die Cloud synchronisiert“, d. h. automatisch auf Server von Plattform-, Betriebssystem-, Anwendungs- oder App-Anbietern übertragen, die in einem Drittland liegen. Das kann eine App wie Whatsapp sein, die Chatverläufe inklusive Texte, Bilder, Filme etc. auf ihren Webservern speichert, oder eine Bildergalerie eines Mobiltelefons, die automatisch synchronisiert wird, damit diese auch auf anderen Endgeräten (oder als Back-up bei Datenverlust) zur Verfügung steht etc. Die von Herrn Smirnow erhobenen Daten könnten schneller als er selbst in Russland ankommen, wenn er einen entsprechenden Dienst auf russischen Servern nutzt. Und wer liest schon die Feinheiten dazu in AGB und prüft, ob dort eine „ordentliche“ Auftragsverarbeitungsvereinbarung enthalten und eine Legitimationsgrundlage für die Übermittlung in Drittländer vorhanden ist? Thematisch ist diese Fallgestaltung auch dafür prädestiniert, Privatpersonen als Verantwortliche zu betreffen (s. oben Fall 18). Mit einer noch „subtileren“ Datenübertragung an die Server von Software-Herstellern beschäftigt sich Fall 36 unten.

Fall 25:
Wen angeben als Empfänger?

Praktischer Fall: Die Huber-Stiftung verfügt über kein eigenes administratives Personal und nimmt die Dienstleistungen einer freiberuflich tätigen Sekretariatskraft, Frau Meier, in Anspruch. Mit Frau Meier hat die Huber-Stiftung eine Auftragsverarbeitungsvereinbarung abgeschlossen. Bewerbungen für neue Mitarbeiter der Huber-Stiftung werden automatisiert an Frau Meier zur Vorsichtung weitergeleitet. Die Huber-Stiftung will die Bewerber im Rahmen ihrer Stellenangebote auf ihrer Internetseite über diese Weiterleitung der Bewerbungen nach Art. 13 Abs. 1 lit. e) DSGVO informieren.

Hier stellt sich vorab schon die Frage, ob eine Auftragsverarbeitungsvereinbarung mit einem Freiberufler nicht zu dessen organisatorischer Eingliederung „in den Auftraggeber" führt, sodass der Freiberufler als „scheinselbstständig" angesehen werden muss. Das würde es erfordern, in einem sozialrechtlichen Statusfeststellungsverfahren feinsinnig zwischen einer allgemeinen Weisungsungebundenheit und einer auf die Verarbeitung personenbezogener Daten beschränkten Weisungsabhängigkeit zu unterscheiden. Arbeitsrechtler warnen jedoch insofern vor jedem noch so kleinen Anhaltspunkt für eine Weisungsabhängigkeit, gleich in Bezug auf was. Die Konsequenz wäre es, das Verhältnis zum Freiberufler bei der Weitergabe von Daten in Richtung eines anderen, eigenständig Verantwortlichen (nämlich den Freiberufler als natürliche Person) zu „drücken", an den die Daten „übermittelt" werden. Dennoch besteht aber zivilrechtlich ein „Auftrag" (Dienstverhältnis bzw. Geschäftsbesorgungsverhältnis), der bei weitem Verständnis des Art. 28 DSGVO (s. oben Fall 7) automatisch zu einer Auftragsverarbeitung führt, die eine Auftragsverarbeitungsvereinbarung notwendig macht.

Darum soll es hier aber nicht vorrangig gehen. Vielmehr sind auch Auftragsverarbeiter – ebenso wie autonome Verantwortliche als Übermittlungsempfänger – „Empfänger", die in Pflichtinformationen angegeben werden müssen (obwohl man auch dies anders sehen kann). Art. 13 Abs. 1 lit. e) DSGVO und Art. 14 Abs. 1 lit. e) DSGVO sprechen genauer von *„die Empfänger oder Kategorien von Empfängern"*, die in den Pflichtinformationen anzugeben sind. Die Frage ist, was diese kryptische Formulierung zu bedeuten hat. Teilweise wird das „oder" im Sinne eines Wahlrechts des Verantwortlichen verstanden. Dies würde bedeuten, dass die Huber-Stiftung sowohl „Empfänger: Frau Ursula Meier" als auch einen Gattungsbegriff wie beispielsweise „freiberufliche Sekretariatskräfte im Wege der Auftragsverarbeitung" verwenden dürfte. Ersteres wäre eventuell Frau Meier nicht recht – ihre personenbezogenen Daten würden öffentlich gemacht – und würde falsch werden, wenn an die Stelle von Frau Meier eine andere freiberufliche Sekretariatskraft treten würde. Letzteres ist zwar inhaltlich

transparenter (verständlicher), aber der Verantwortliche kennt natürlich den Namen des konkreten Empfängers und könnte diesen auch angeben.

Teilweise wird allerdings auch argumentiert, dass in jedem Fall der „Empfänger" anzugeben ist, während die Angabe der Kategorie freigestellt ist. So nennt der „gesetzesgleiche" Erwägungsgrund 63 ausschließlich „die Empfänger der personenbezogenen Daten" als besonders wichtige Information, nicht aber die Kategorien. Dies würde bedeuten, dass die Huber-Stiftung entweder „Empfänger: Frau Ursula Meier" oder aber „Empfänger: Frau Ursula Meier (als freiberufliche Sekretariatskraft im Wege der Auftragsverarbeitung)" schreiben dürfte.

Wurde Frau Meier namentlich angegeben, so ist die weitere Frage zu beantworten, ob dem Betroffenen gegenüber eine Änderung mitzuteilen ist, wenn Frau Meier ausscheidet bzw. ersetzt wird, weil dann die ursprünglichen Pflichtinformationen „falsch" geworden sind. Solange der Verarbeitungszweck sich nicht ändert, soll eine solche Informationspflicht nur in Ausnahmefällen bestehen. Für den Wechsel eines Empfängers, welcher derselben Kategorie (hier also „freiberufliche Sekretariatskräfte im Wege der Auftragsverarbeitung") angehört, muss keine Neuinformation stattfinden. Wenn aber der Charakter des Umgangs mit den betroffenen Daten „fundamental" geändert wird, etwa bei Einsatz einer Outsourcing-Lösung in einem unsicheren Drittland (Frau Meier wird durch eine indische Sekretariatskraft mit Online-Zugriff auf die Systeme der Huber-Stiftung ersetzt), muss (angeblich) eine Neuinformation der Betroffenen erfolgen. Das Etablieren entsprechender unternehmensinterner Prozesse, die derartige Veränderungen identifizieren und entsprechende „Nachinformationen" an die Betroffenen senden, dürfte durchaus anspruchsvoll sein.

Wenn man diesen Fall „extrapoliert", kann man sich leicht vorstellen, wie viele Empfänger in verschiedenen Verarbeitungssituationen (ggf. namentlich) angegeben werden müssten, zumal die Weitergabe der Daten an einen ursprünglich in den Pflichtinformationen nicht genannten Empfänger stets noch die Frage der Zweckänderung (und einer entsprechenden Zweckänderungsnachricht an den Betroffenen) aufwirft. Gerade Beschäftigtendaten werden in großem Stil an Dritte weitergegeben, seien es Steuerberater, Ämter, Sozialversicherungsträger (einschließlich Berufsgenossenschaften), Betriebsärzte, eine Konzern-Rechtsabteilung etc. Vor diesem Hintergrund müsste man als Verantwortlicher eigentlich an einen „Datenexportprozess" bei der Übermittlung jeglicher personenbezogener Daten an Dritte denken, in dessen Rahmen strukturiert geprüft wird, ob der Dritte, an den übermittelt werden soll, ein schon (materiell im Sinne einer Legitimationsgrundlage und formell im Sinne einer Benennung als Empfänger) „legitimierter" Dritter ist und wenn nicht, welche Folgen (bzw. weiteren Prozessschritte) dies auslösen muss.

Fall 26:
Das ist mal wieder nicht typisch!

Praktischer Fall: In datenschutzrechtlichen Pflichthinweisen, welche die Huber AG standardmäßig ihren E-Mails beifügt, heißt es „Für den Fall, dass wir mit Ihrem Arbeitgeber in einem vertraglichen Verhältnis stehen, gilt Folgendes: [...] Für den Fall, dass wir Sie als natürliche Person als Direktmarketing-Kontakt führen, gilt Folgendes: [...] Für den Fall, dass weder Sie noch ihr möglicher Arbeitgeber bislang in einem Verhältnis zur Huber AG standen, gilt Folgendes: [...]". Herr Schulze schreibt eine Dissertation zum Thema „Wie gehen Unternehmen mit Datenschutz um?" und hat auf einer Veranstaltung Frau Müller, Leiterin der Rechtsabteilung der Huber AG, kennengelernt. Nun wendet er sich mit einem Fragebogen an Frau Müller in der Hoffnung, dass diese ihn „pro bono" bei seiner Feldforschung unterstützen kann. In seiner E-Mail gibt er seine private Adresse und Telefonnummer an. Frau Müller befindet sich zu dieser Zeit in Urlaub, sodass Herr Schulze eine Abwesenheitsnotiz mit dem Hinweis, dass sich ihre Vertretung um die Angelegenheit kümmern werde, verbunden mit den obigen Pflichthinweisen, erhält. Kurz darauf erhält Herr Schulze noch eine Nachricht von der Vertretung von Frau Müller, Frau Lehmann, dass sie sich die Unterlagen angesehen habe, aber dazu nichts sagen könne, sodass Herr Schulze bitte auf die Rückkehr von Frau Müller warten möge. Auch diese E-Mail enthält die obigen Pflichthinweise.

Der Fall beginnt damit, dass Pflichthinweise im Grundsatz bedingungsfeindlich sind. Nur dem Gesetzgeber steht es zu, die Subsumtionslast auf die Gesetzesadressaten abzuwälzen. Letztere dürfen diese nicht weiter auf die „heilige Kuh des Datenschutzrechts", den Betroffenen, abwälzen. Vielmehr müssen die Verantwortlichen den Kopf für eine falsche Einordnung hinhalten. Warum soll es ihnen besser ergehen als den „Verwendern" von AGB, die ja auch transparent, verständlich und klar sein müssen, wie es Art. 12 Abs. 1 DSGVO für die Pflichthinweise vorschreibt? Man kann also – auch wenn das für das Pendant der AGBs nicht uneingeschränkt gilt – mit gutem Grund behaupten, dass „verzweigende" bzw. „konditionale" Pflichthinweise die Voraussetzungen der DSGVO nicht erfüllen, selbst wenn der Betroffene den richtigen „Pfad" solcher Verzweigungen in seiner konkreten Situation durchaus gut beurteilen könnte. Auch dass dieses Urteilsvermögen in besonderer Weise gegeben sein sollte, wenn der „typische" Betroffene der Repräsentant eines Unternehmens ist und dem Verantwortlichen in dieser Eigenschaft gegenübertritt („unternehmerischer Verkehr"), wird wohl wenig helfen.

➢ Datenverarbeitung ohne gehörige Pflichtinformationen

Ergänzend ist an dieser Stelle einzuflechten, dass unklar ist, ob bzw. unter welchen Umständen personenbezogene Daten, die unter Verstoß gegen die Informationspflichten der Art. 13 und 14 DSGVO erhoben wurden, als solche rechtswidrig („toxisch") sind und nicht weiter verarbeitet werden dürfen. Dann wären auch sämtliche späteren Verarbeitungshandlungen – auch bei Dritten, an die die Daten weiterübermittelt wurden – rechtswidrig.

Eine kleine Passage des in Fall 1 erwähnten EuGH-Urteils vom Oktober 2015 könnte dahingehend zu verstehen sein: Die (ordnungsgemäße) Erfüllung der Informationspflicht soll danach die „Voraussetzung" für die weitere Verarbeitung der übermittelten Daten sein. Dies wird aber „landläufig" nur so verstanden, dass eine solche „Infizierung" der erhaltenen Daten nur dann infrage kommt, wenn die Verarbeitung gegenüber dem Betroffenen „vollkommen intransparent" ist, was immer das heißt, bzw. wenn dem Betroffenen eine Pflicht zur Bereitstellung der Daten vorgegaukelt oder eine Einwilligung des Betroffenen erschlichen wurde. Andere Autoren unterscheiden nach der Legitimationsgrundlage: Liegt eine gesetzliche Verpflichtung vor (Art. 6 Abs. 1 S. 1 lit. c DSGVO), sollen auch die unter Verstoß gegen Informationspflichten erhobenen Daten weiterverarbeitet werden dürfen (bzw. müssen), während dies im Falle einer Einwilligung nicht zulässig wäre.

➢ Der ideale Verantwortliche weiß alles schon vorher

Was nun die verzweigenden und deshalb möglicherweise „unrichtigen" Pflichthinweise als solche angeht, so weiß natürlich jeder, der sich mit der Realität beschäftigt, dass es nicht immer so einfach ist, diese in standardisierte (Unternehmens-) Abläufe zu pressen. Entsprechend schwierig ist es, die von der DSGVO aufgestellte strikte Forderung nach einer unbedingt richtigen Behandlung jeder einzelnen Fallgestaltung zu erfüllen, zumal vor dem Hintergrund aller bestehenden datenschutzrechtlichen Bewertungs- und Einordnungs-Unschärfen. Wie sich der Europäische Datenschutzausschuss das Vorgehen vorstellt, kann einem „Beispielsfall" in dessen Empfehlungen vom November 2019 zum Thema „*privacy by design/by default*" entnommen werden:

„A controller is designing a privacy policy in order to comply with the requirements of transparency. The privacy policy cannot contain a lengthy bulk of information that is difficult for the average data subject to penetrate and understand, it must be written in clear and concise language and make it easy for the user of the website to understand how their personal data is processed. The controller therefore provides information in a multi-layered manner, where the most important points are highlighted. Drop-down menus and links to other pages are

provided to further explain the concepts in the policy. The controller also makes sure that the information is provided in a multi-channel manner, providing video clips to explain the most important points of the information. The privacy policy cannot be difficult for data subjects to access. The privacy policy is thus made available and visible on all internal web-pages of the site in question, so that the data subject is always only one click away from accessing the information. The information provided is also designed in accordance with the best practices and standards of universal design to make it accessible to all. Moreover, necessary information must also be provided in the right context, at the appropriate time. This means, that generally a privacy policy on the website alone is not sufficient for the controller to meet the requirements of transparency. The controller therefore designs an information flow, presenting the data subject with relevant information within the appropriate contexts using e.g. informational snippets or pop-ups. For example, when asking the data subject to enter personal data, the controller informs the data subject of how the personal data will be processed and why that personal data is necessary for the processing."

Ganz einfach, oder? Doch die wohl hier durchscheinende Annahme, der Verantwortliche könne im Vorhinein selbst bei „offenen Kommunikationskanälen mit ungewissem Input" alles wissen, was für die Pflichthinweise relevant ist, wird sogar von der DSGVO selbst in Zweifel gezogen: Art. 21 Abs. 1 DSGVO enthält eine Textpassage in Bezug auf Interessenabwägungen, die nahelegt, dass eine „typisierte Betrachtung" durch den Verantwortlichen sich im Nachhinein „aus Gründen, die sich aus der besonderen Situation" des Betroffenen ergeben, als falsch herausstellen kann. War in diesem Fall die ursprünglich vorgenommene typisierte Interessenabwägung, die sich durch einen Widerspruch und das Vorbringen des Betroffenen zu seiner „besonderen Situation" nun als im Einzelfall objektiv unrichtig herausstellt, schon von Anfang an „falsch"? Der DSGVO kann man diesen Schluss eigentlich nicht entnehmen, im Gegenteil: Gerade der hier vorgesehene „Korrekturmechanismus" der DSGVO im Rahmen der Interessenabwägung impliziert, dass die ursprüngliche Interessenabwägung – und damit auch der entsprechende Pflichthinweis – typisiert erfolgen durfte. Sonst hätte auch die Interessenabwägung als Fall der mutmaßlichen Einwilligung, die ja begrifflich gerade in Abwesenheit des Betroffenen erfolgt, gar keinen Sinn: Man müsste mit dem Betroffenen vorab dessen Interessen und „besondere Situation" erörtern und kann dann auch gleich dessen ausdrückliche Einwilligung einholen (siehe dazu oben Fall 17).

In diesem Zusammenhang am Rande noch die Anmerkung, dass die Datenschutzkonferenz in ihrer „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien" vom März 2019 der Auffassung ist, die Einräumung „überobligatorischer Widerspruchsrechte", d. h.

eines nicht an die Voraussetzungen des Art. 21 Abs. 1 DSGVO geknüpften jederzeit möglichen Widerspruchsrechts (wie im Falle des Art. 21 Abs. 2 DSGVO), könne bei der Abwägung im Rahmen der Interessenabwägung selbst ein Argument zugunsten des Verantwortlichen darstellen. Ähnliches gilt übrigens nach dem bayerischen Landesamt für Datenschutzaufsicht in seinem Tätigkeitsbericht 2017/2018 für besondere technische Vorkehrungen (Datenschutz durch Technikgestaltung) und für die Ausgestaltung der Sicherheit der Verarbeitung: Ein besonders guter Schutz der Daten streitet für die Interessenabwägung zugunsten des Verantwortlichen.

- Prognose misslungen

Das Problem dieses Falles geht aber über die Frage von Pflichthinweisen, welche die Besonderheiten der konkreten Erhebungssituation nicht individuell berücksichtigen, hinaus. Vorliegend wurde im Rahmen des Designs eines „Autoreply"-Prozesses im Unternehmen von drei „typischen Fällen" von Eingaben von Betroffenen ausgegangen, dann aber eine untypische E-Mail eingesandt, an die im Zuge des Prozessdesigns nicht gedacht wurde. Die Huber AG kann daher im Streitfall keine technischen und organisatorischen Maßnahmen nachweisen (Art. 24 Abs. 1 DSGVO), die sicherstellen, dass die individuelle Erhebungssituation (auf Basis der ihr jeweils vorliegenden konkreten, wenngleich möglicherweise lückenhaften Informationen) gemäß der DSGVO behandelt wird. Die Huber AG hat einfach nur „ihren Standardprozess darüber laufen lassen". Was wäre aber nun auf dieser „systemischen Compliance-Ebene" („systems and controls") richtig gewesen? Dürfte die Huber AG, um die DSGVO in jedem Fall richtig zu erfüllen, keine datenschutzrechtlichen Pflichthinweise in einen E-Mail-Disclaimer aufnehmen? Müsste sie nicht vielmehr – je nach Größe – eine Vielzahl von „DSGVO-Spezialisten" einstellen, die bei jeder eingehenden E-Mail erst einmal untersuchen, welche personenbezogenen Daten dort zu welchen Zwecken und in welchem Kontext enthalten sind, welche Legitimationsgrundlagen gegeben sind etc. (siehe dazu auch oben Fall 2), um dann Pflichthinweise für den Absender individuell zu fertigen? Lässt sich dieser individuelle Prozess (dereinst) anhand des Inhalts der empfangenen E-Mail durch Algorithmen aus dem Bereich der vielgerühmten künstlichen Intelligenz automatisieren?

Vermutlich wird man den Fall über die der DSGVO immanente Risikoabwägung lösen müssen. Denn sämtliche konkreten Pflichten des Verantwortlichen sind letztlich *„unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen"* zu ermitteln (Art. 24 Abs. 1 DSGVO). Einerseits ist also sicherzustellen und der Nachweis dafür zu erbringen, dass die Verarbeitung gemäß der DSGVO erfolgt, andererseits sind die Maßnahmen dafür relativ anhand der Risikogeneigtheit

zu definieren. Was passiert also, wenn dabei etwas „durchs Raster fällt"? Ist dann die mindere Risikogeneigtheit – nur, aber immerhin – ein Argument beim späteren Nachweis des Verantwortlichen, *„dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist"* (Art. 82 Abs. 3 DSGVO)?

Fall 27:
Warte mal mit der Wartung

Praktischer Fall: Die Huber AG hat bei der Maier GmbH eine Mehrplatz-Lizenz für eine Personalverwaltungssoftware erworben und dabei auch einen entsprechenden Wartungsvertrag abgeschlossen. Wenn im Rahmen der Wartung Fehler gemeldet werden, die für die Maier GmbH nicht nachvollziehbar sind, erhält der zuständige Programmierer der Maier GmbH einen Live-Bildschirmzugriff auf den PC des zuständigen Mitarbeiters der Personalabteilung der Huber AG. Der zuständige Mitarbeiter der Huber AG kann dann das Problem „vorführen" und kommentieren. Die Huber AG verlangt von der Maier GmbH den Abschluss einer Auftragsverarbeitungsvereinbarung, da die Maier GmbH durch diese „Vorführungen" mit sensiblen Personaldaten der Huber AG in Berührung kommt und theoretisch auch einen „Screenshot" der gezeigten Inhalte anfertigen könnte. Die Maier GmbH weigert sich, eine solche Auftragsverarbeitungsvereinbarung abzuschließen, da sie Software entwickelt und keine Daten der Huber AG im Auftrag verarbeitet. Die Huber AG überlegt, ob sie die Maier GmbH in ihren Pflichtinformationen für ihre Beschäftigten als „Empfänger" für deren personenbezogene Daten angibt.

Das (zumindest in dieser Hinsicht) gute, alte BDSG enthielt vor dem Inkrafttreten der DSGVO in den Regelungen über die Auftragsverarbeitung (damals noch „Auftragsdatenverarbeitung") einen Satz, wonach diese Regelungen entsprechend Anwendung finden,

„wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann".

Der Gesetzgeber war damals also zumindest der Meinung, dass nicht hinreichend sicher war, ob eine Software-Wartung nun eine Auftragsverarbeitung ist oder nicht, und ordnete vorsorglich die Anwendbarkeit der entsprechenden Regelungen an. Echte Methodiker werden natürlich sagen, dass der Gesetzgeber gerade davon ausging, dass Software-Wartung begrifflich keine Auftragsverarbeitung ist, denn sonst hätte es der Anordnung der analogen Anwendung gar nicht bedurft. Aber das spielt heute keine Rolle mehr.

➢ Unterschiedliche Rechtsauffassungen

In der DSGVO ist Auftragsverarbeitung einfach Auftragsverarbeitung. Wer personenbezogene Daten im Auftrag verarbeitet, ist Auftragsverarbeiter (s. o. Fall 7). Und wer einen Dienstleister einsetzt und ihm personenbezogene Daten zur Verfügung stellt, ohne mit ihm eine Auftragsverarbeitungsvereinbarung abgeschlossen zu haben, der begeht einen DSGVO-Verstoß.

Nach einer Entscheidung der Hamburger Datenschutzbehörde aus dem Januar 2019 hat (natürlich) der Verantwortliche die Pflicht, eine Auftragsverarbeitungsvereinbarung mit dem Dienstleister abzuschließen. Weigert sich der Dienstleister, eine solche Vereinbarung vorzulegen oder abzuschließen, kann man nicht einfach „zur Tagesordnung übergehen" und die personenbezogenen Daten „vertragslos" weitergeben. Die Anregung der Datenschutzbehörde an den Verantwortlichen, einen solchen Vertrag selbst zu verfassen und dem Dienstleister (in „seiner Sprache" – im dortigen Fall spanisch) „ultimativ" zur Unterschrift zu übersenden, wird in der Praxis daran scheitern, dass die im Vertrag gewöhnlich aufzuführenden technischen und organisatorischen Maßnahmen des Dienstleisters zur Sicherung der auftrags- und gesetzesgemäßen Datenverarbeitung dem Auftraggeber zu diesem Zeitpunkt nicht bekannt sein werden. Es wäre zwar nach Abschluss der Vereinbarung die Pflicht des Verantwortlichen, diese Maßnahmen des Dienstleisters zu prüfen, aber was man noch nicht kennt, kann man weder beschreiben noch prüfen. Der Dienstleister hat sich in diesem Fall also selbst „disqualifiziert". Die mangelnde Bereitschaft zur Vorlage und/oder zum Abschluss einer Auftragsverarbeitungsvereinbarung führt also dazu, dass der Dienstleister entweder nicht eingesetzt werden darf oder seine Aufgaben so zugeschnitten bzw. umformuliert werden, dass er im Rahmen der Dienstleistung keine personenbezogenen Daten erhält. Das bayerische Landesamt für Datenschutzaufsicht formuliert dies in seinem Tätigkeitsbericht 2017/2018 so:

„Können sich ein Verantwortlicher und ein Auftragsverarbeiter nicht auf den Abschluss oder eine erforderliche Anpassung der Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO verständigen, weil sich z. B. der Auftraggeber weigert, den Vertrag abzuschließen oder einen nach altem Recht bestehenden Vertrag anzupassen, entfällt für den Auftragsverarbeiter die datenschutzrechtliche Grundlage für die Verarbeitung. Daran ändert sich auch dann nichts, wenn Auftraggeber und Auftragnehmer dem gleichen Konzern angehören und/oder dadurch bspw. für Beschäftigte des Auftraggebers oder andere juristische oder natürliche Personen keine Leistungen durch den Auftraggeber erbracht werden können."

➢ Wartung als Auftragsverarbeitung?

Die entscheidende Frage im vorliegenden Fall ist nun, ob Software-Wartung Auftragsverarbeitung ist, wenn die Möglichkeit besteht, dabei personenbezogene Daten zur Kenntnis zu nehmen. Dies ist natürlich bei Vor-Ort-Besuchen der Fall, wenn der Mitarbeiter des Softwareherstellers „mal mit auf den Bildschirm schaut". Aber auch im Rahmen der Fernwartung ist dies möglich und der Mitarbeiter des Softwarehersteller kann in diesem Fall sogar unbemerkt einen Screenshot anfertigen und die darauf enthaltenen personenbezogenen Daten auswerten (s. auch o. Fälle 23 und 24). Zusätzlich stellt sich die Frage, ob der Softwarehersteller, auch wenn unbekannt ist, ob und wie oft eine Wartung erfolgt und welche personenbezogenen Daten dabei eingesehen werden (können), als „Empfänger" der personenbezogenen Daten in den Pflichthinweisen an den Betroffenen angegeben werden muss.

Soweit sich die Juristen bislang mit dem Fortbestand der alten Regel aus dem BDSG beschäftigen, gehen sie überwiegend davon aus, dass Software-Wartung unter den Begriff der Auftragsverarbeitung im Sinne der DSGVO fällt. Begründet wird dies mit der „weiten" begrifflichen Formulierung der Auftragsverarbeitung in der DSGVO. Man kann das überzeugend finden oder auch nicht (s. dazu auch oben Fall 7). Auch die Datenschutzkonferenz führt in ihrem Kurzpapier Nr. 13 zum Thema Auftragsverarbeitung im Kapitel „Wartung und Fernzugriffe" sinngemäß aus: Da definitionsgemäß jedes „Auslesen, Abfragen, Verwenden" personenbezogener Daten eine „Verarbeitung" sei, sei jeder, der so etwas im Rahmen eines Auftragsverhältnisses macht (oder auch nur machen kann), ein Auftragsverarbeiter. Nur *„bei einer rein technischen Wartung der Infrastruktur einer IT durch Dienstleister (z. B. Arbeiten an Stromzufuhr, Kühlung, Heizung)"* scheide diese Qualifizierung aus – mutmaßlich, weil die Datenschutzkonferenz annimmt, dass bei diesen Arbeiten kein Risiko der Einsichtnahme in personenbezogene Daten besteht. Die Frage, ob die Verarbeitung personenbezogener Daten den Kernbereich der Dienstleistung ausmacht oder eine mechanische Verarbeitung als „verlängerte Werkbank" vorliegt, spielt keine Rolle mehr. Mit anderen Worten: Ohne weitergehende Erklärungen gehen die Datenschutzbehörden davon aus, dass jedes „Einsehen-Können" personenbezogener Daten, auch wenn dies ausdrücklich gerade nicht mit dem Auftrag bezweckt (bzw. vertragsgemäß) ist, zu einem Auftragsverarbeitungsverhältnis führt.

Nun würde sich auf dieser Basis natürlich wieder die Frage der begrifflichen Grenze stellen, also wie wahrscheinlich bzw. absehbar eine solche Einsichtnahmemöglichkeit sein muss. Auf Basis des Grundsatzes „nachher ist man immer schlauer" (englisch: „with the benefit of hindsight") wird wohl so manche zufällige bzw. ungeplante Kenntnisnahme in der Rückschau als „natürlich vorhersehbar" eingestuft werden. Wenn also ein Gärtner um eine Ter-

rasse herum den Garten (als Hardware) „wartet“ und auf der Terrasse oft über die Gesundheitsprobleme von „Tante Marta“ gesprochen werden – muss dann eine Auftragsverarbeitungsvereinbarung mit dem Gärtner abgeschlossen werden oder genügt es, wenn der Gärtner zusichert, dass er bei der Arbeit Ohrenstöpsel trägt? Aber selbst neben diesem plakativen Beispiel gibt es ja bekanntlich viele Dienstleister, die die Gelegenheit haben, nebenbei personenbezogene Daten zu „erhaschen“. Das fängt mit dem Reinigungspersonal an und endet bei den Fensterputzern und Monteuren noch lange nicht. Schwierig wird es auch, wenn man mit den betreffenden Dienstleistungen gar nicht selbst in vertraglichem Kontakt steht – etwa wenn die vom Vermieter beauftragten Handwerker in den gemieteten Geschäftsräumen tätig sind und dabei mit personenbezogenen Daten, die der Mieter verarbeitet, in Berührung kommen. Unter dem alten BDSG hat man sich – eben wegen der begrenzten „entsprechenden“ Anwendbarkeit der Regelungen für die Auftrags(daten)verarbeitung auf „die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen“ – in der Regel damit beholfen, in diesen Fällen eine Geheimhaltungsvereinbarung abzuschließen. Letztlich ging es dabei darum, den Dienstleister zur verpflichten, bei Ausführung seiner Tätigkeiten von personenbezogenen Daten „nicht Kenntnis zu nehmen“, und wenn es doch einmal „passiert“, diese Informationen für nichts zu verwenden und diese nicht weiterzugeben (also so zu tun, als hätte er die Information nicht zur Kenntnis genommen). Muss man nun in allen diesen Fällen eine Auftragsverarbeitungsvereinbarung treffen und der Dienstleister muss seine technischen und organisatorischen Maßnahmen beschreiben?

- „Anonymisierung“ der Wartung

Man kann sich nun überlegen, wie eine Software-(Fern-)Wartung so ausgestaltet werden kann, dass keine Möglichkeit besteht, Einblick in personenbezogene Daten zu nehmen. Der Mitarbeiter des Unternehmens, das die Software einsetzt, könnte selbst Screenshots anfertigen – hoffentlich hat er ein „need to know“ in Bezug auf diese Daten – und in diesen Screenshots sämtliche personenbezogenen Daten anonymisieren bzw. schwärzen. Dies erhöht natürlich den Aufwand aufseiten des die Software nutzenden Unternehmens beträchtlich. Und auf der anderen Seite macht es die Software-Wartung umständlicher: Die geschwärzten Daten werden häufig nicht mehr gleichermaßen aussagekräftig sein und der Mitarbeiter des Software-Herstellers kann nicht interaktiv „mal schnell hier klicken, um zu sehen, was dann passiert“. Eine weitere Alternative – „privacy by design“ lässt grüßen – wäre es, in die Software einen Fernwartungs-Modus zu integrieren, bei dem sämtliche Inhaltsdaten automatisch „verwirbelt“ (anonymisiert), (teil-)geschwärzt oder durch Testdaten ersetzt werden, die keinen Bezug zu natürlichen Personen haben. Für den Softwarehersteller erscheint da doch der Abschluss einer Auftragsverarbeitungsvereinbarung als das kleinere Übel – während der Verantwortliche „eigentlich“ im Rahmen einer Beschaffungsentscheidung

und im Rahmen des Zumutbaren einen Hersteller vorziehen müsste, der die Wartung so gestaltet, dass gar keine personenbezogenen Daten an ihn übertragen werden.

Fall 28:
Löschen nur auf Anforderung?

Praktischer Fall: Die Huber AG verfügt über Altbestände von Unternehmensdaten (E-Mails, Dokumente, Korrespondenz, Buchhaltungsunterlagen etc.), deren Inhalt sie selbst nicht so genau kennt („irgendwo liegt irgendwas"). Mit absoluter Sicherheit sind auch personenbezogene Daten darunter, zumindest von Mitarbeitern der Huber AG, aber auch von Mitarbeitern anderer Unternehmen, mit denen die Huber AG einmal in Geschäftsbeziehung stand oder noch steht. Eine Löschung kommt für den Vorstand nicht in Frage, weil „man die Daten dann nicht mehr hat, wenn man sie noch mal braucht".

Ein Schelm, der denkt, dass es in Zeiten der DSGVO solche (mittelständischen) Unternehmen nicht (mehr) gibt. Es mag allerdings überraschen, dass über die Frage, ob datenschutzrechtlich eine Löschpflicht des Verantwortlichen auch ohne Aufforderung durch den Betroffenen besteht, unter Juristen überhaupt diskutiert wird. Den Datenschutzbehörden stehen dabei natürlich die Haare zu Berge: Personenbezogene Daten, deren Erhebungs- bzw. Verarbeitungszweck erreicht oder weggefallen ist, müssen doch gelöscht werden, egal, ob das Betroffene verlangt oder nicht! So ausdrücklich auch das bayerische Landesamt für Datenschutzaufsicht in seinem Tätigkeitsbericht 2017/2018. Und gerade dafür gibt es in der DSGVO auch die Grundsätze der Zweckbindung, der Speicherbegrenzung und der Datenminimierung. Außerhalb der DSGVO gibt es ergänzend beispielsweise die DIN 66398 für Löschkonzepte, mit deren Hilfe automatische Löschroutinen, zumeist softwarebasiert, parametrisiert werden können. Diese Norm kann gleichwohl nur eine erste Näherung ermöglichen, denn die Einordnung eines Datentyps in die „nächsthöhere" Fristenkategorie würde aus der (Einzelfallbetrachtungs-)Perspektive der DSGVO zu einer möglicherweise unzulässig fortdauernden Speicherung führen.

➢ Was sagt der Gesetzestext?

Man kann dennoch die Frage stellen, ob sich die Löschpflicht ohne Anforderung nur aus diesen etwas „luftigen" Prinzipien der DSGVO ergibt oder ob der Gesetzestext, wenn es dem Gesetzgeber denn so wichtig wäre, eine konkrete und „aufforderungsunabhängige" Pflicht des Verantwortlichen formuliert. Die Löschung personenbezogener Daten wird in der DSGVO nur in Art. 17 ausdrücklich angeordnet. Diese Vorschrift enthält einen bemerkenswert zweideutigen Satzeingang:

„Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:"

Die Preisfrage ist nun, ob dies sprachlich als „A hat das Recht, von B etwas zu verlangen, und *deshalb* muss B das dann auch tun" – also als Tautologie – zu lesen ist oder als „A hat das Recht, von B etwas zu verlangen, aber *auch unabhängig davon* muss B das tun" zu lesen ist. Die Auswirkungen sind natürlich erheblich. Wie viele Betroffene wissen gar nicht – Aufklärung und Informationspflichten hin oder her –, wer alles welche personenbezogenen Daten über sie hat. Die Betroffenen wären nie in der Lage, sämtliche Verantwortliche, denen sie irgendwann ihre personenbezogene Daten „gegeben" haben, im Nachhinein zu benennen. Auch kostet es zumindest Zeit und Nerven, Löschverlangen an all diese Verantwortlichen zu senden. Wenn es also für die Löschung eines Löschverlangens bedürfte, wäre die „Dunkelziffer" der personenbezogenen Daten, die (sehr) viele Verantwortliche dann „einfach so" schlummern lassen könnten – weil ja die Betroffenen ihre Löschung nicht verfolgen –, wohl jetzt schon gigantisch und noch dazu exponentiell anwachsend. Und warum sollte der Gesetzgeber zwei Seiten derselben Medaille – die Berechtigung des einen und die spiegelbildliche Verpflichtung des anderen – überflüssigerweise in einen Satz packen? Auch beim Berichtigungsanspruch (Art. 16 DSGVO) heißt es beispielsweise „Die betroffene Person hat das Recht, von dem Verantwortlichen die Berichtigung [...] zu verlangen", ohne dass hier noch „und der Verantwortliche ist verpflichtet, die Berichtigung vorzunehmen" folgt.

- Kostenloser Cloud-Speicher für alle?

Gegen die „aufforderungsunabhängige" Löschpflicht wird gleichwohl ins Feld geführt, dass viele Löschungen, die ansonsten „automatisch" – also vom Betroffenen unbemerkt – geschehen müssten, dem Betroffenen vielleicht gar nicht recht wären. Dies beruht darauf, dass die DSGVO insbesondere im Bereich der Einschränkung der Verarbeitung (Art. 18) ein „Recht auf kostenloses Speichern" enthält: Der Betroffene kann (anstelle der Löschung) verlangen, dass die Daten für eng begrenzte Zwecke, praktisch „für den Betroffenen", vorgehalten werden müssen. Einen solchen „kostenlosen Back-up-Dienst" hätte man wohl zu Zeiten knappen Speicherplatzes nicht gewagt in ein Gesetz zu schreiben. Entsprechend wird argumentiert, dass der Verantwortliche, wenn er Daten ohne Anforderung des Betroffenen löschen möchte, vorher den Betroffenen fragen müsse, da dieser vielleicht sein Recht auf Einschränkung der Verarbeitung geltend machen will (sodass die Daten nicht mehr einfach so gelöscht werden dürfen). Es genügt also danach nicht schon, ein möglichst vollständiges Löschkon-

zept zu haben – es müssen auch noch sämtliche Betroffenen erreicht und ihre Antwort abgewartet werden. Und sämtliche Betroffenen würden permanent dadurch „belästigt", dass Verantwortliche fragen, ob es genehm ist, dass nun dieser oder jener Datensatz gelöscht wird. Da dürfte man eigentlich erwarten, dass eine so grundsätzliche und in der Praxis extrem ressourcenintensive „Löschfragepflicht" im Gesetz ausdrücklich geregelt wird. So abwegig ist die Annahme einer solchen Pflicht aber nicht, denn schließlich hält der Europäische Datenschutzausschuss in Empfehlungen vom November 2019 zum Thema *„privacy by design/by default"* unter dem Stichwort „notwendige Schutzmaßnahmen" (*„necessary safeguards"*, in der deutschen DSGVO-Übersetzung missverständlich als „notwendige Garantien" bezeichnet) auch Aufbewahrungserinnerungen (*„retention reminder"*) für notwendig, damit der Betroffene intervenieren kann:

„Enabling data subjects to intervene in the processing, providing automatic and repeated information about what personal data is being stored, or having a retention reminder in a data repository may be examples of necessary safeguards."

Ebenfalls in diese Richtung geht ein Bescheid der österreichischen Datenschutzbehörde vom Dezember 2018, wonach die Löschung der gesamten personenbezogenen Daten des Betroffenen – trotz nur partiellen Löschungsantrages – nicht „der Verwendung von Daten nach Treu und Glauben entspricht", da so die „Integrität des Datensatzes nachhaltig beeinträchtigt" wurde. Man sieht hier, dass ein Verbot der Löschung ohne Anforderung auch auf Umwegen hergeleitet werden kann. Und auch das bayerische Landesamt für Datenschutzaufsicht schränkt seine oben zitierte Äußerung in Richtung „aufforderungsloser" Löschung wie folgt ein:

„Sollte für die Erreichung des Zwecks, für den die Daten erhoben wurden, die Aufbewahrung noch notwendig sein, muss bzw. darf nicht gelöscht werden. Dies kann insbesondere dann der Fall sein, wenn die Gesundheitsdaten wichtige Informationen enthalten, von denen davon ausgegangen werden kann, dass für diese auch nach Ablauf gesetzlicher Aufbewahrungsfristen das Interesse des Berechtigten an der Speicherung das an der Löschung überwiegt, bspw. im Hinblick auf Medikamentenunverträglichkeiten."

Ob dies nur für die vom bayerischen Landesamt dann exemplarisch zitierten gesetzlichen Aufbewahrungspflichten (hier § 630f Abs. 3 BGB) gilt oder ganz allgemein, bleibt offen. Jedenfalls stellt sich die Folgefrage, ob der Verantwortliche nun Hellseher werden soll („davon ausgegangen werden kann") oder sich immer mal wieder mit sämtlichen Betroffenen,

deren Daten er verarbeitet, darüber austauschen soll, was sie denn nun in Bezug auf ihre Daten gerne hätten.

Auch hier lässt sich also nicht mehr sagen, dass es einen klaren Trend in dieser Frage gibt. Hätte das der Gesetzgeber nicht klarer formulieren sollen?

➢ Muss immer bei Wegfall der Legitimationsgrundlage gelöscht werden?

In der Kommentarliteratur zu Art. 17 DSGVO heißt es, dass *„die Löschung immer dann zu erfolgen hat, wenn die Verarbeitung der betreffenden personenbezogenen Daten bereits rechtswidrig war oder in Zukunft rechtswidrig sein wird"*. Das würde im Prinzip bedeuten, dass der Wegfall einer Legitimationsgrundlage die Daten „löschpflichtig" macht. So steht es allerdings nicht in Art. 17 Abs. 1 DSGVO, der explizit anordnet, dass eine Löschung nur dann vorgenommen werden muss, „sofern einer der folgenden Gründe zutrifft", und dazu zählt nicht der Wegfall eines Legitimationsgrundes bzw. das „Rechtswidrig-Werden" der Verarbeitung. Im Gegenteil: In Buchstabe d) heißt es explizit in der Vergangenheitsform *„Die personenbezogenen Daten wurden unrechtmäßig verarbeitet"*, d. h. es lag bereits ein Verstoß gegen Datenschutzrecht vor. Ausdrücklich regelt Art. 17 DSGVO nur den Wegfall zweier Legitimationsgrundlagen. Dies ist einerseits die Einwilligung (Art. 17 Abs. 1 lit. b DSGVO), für deren Widerruf die DSGVO hier selbst anordnet, dass nur dann gelöscht werden muss, wenn *„es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt"* (s. aber oben Fall 8 aus der Perspektive der Erhebung). Andererseits findet sich hier die Interessenabwägung und die erfolgreiche Widerspruchseinlegung (Art. 17 Abs. 1 lit. c DSGVO) – hier nicht mit der „Rückgriffsklausel" auf eine mögliche andere Legitimationsgrundlage.

Ansonsten findet sich in Art. 17 Abs. 1 DSGVO gerade nicht der Grundsatz, dass gelöscht werden muss, wenn die Legitimationsgrundlage entfällt, sondern dann, wenn *„die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind"* (Art. 17 Abs. 1 lit. a DSGVO). Gibt es nun einen Unterschied zwischen Zweckerfüllung bzw. Zweckfortfall und Wegfall der Legitimationsgrundlage? Kann z. B. ein Zweckfortfall vorliegen, auch wenn ein Vertrag, der Legitimationsgrundlage war bzw. ist, noch besteht? Kann umgekehrt ein Vertrag als Legitimationsgrundlage entfallen, aber die Daten dennoch für den ursprünglichen Erhebungszweck (weiter) notwendig sein? Man mag das für akademische Spitzfindigkeiten halten, aber es zeigt, dass die Begrifflichkeiten in den entscheidenden Artikeln 6 (Legitimationsgrund) und 17 (Recht auf Löschung) DSGVO nicht vollständig synchronisiert wurden.

➢ Was heißt das eigentlich: Löschen?

Wie auch immer: Soll bzw. muss dann irgendwann tatsächlich gelöscht werden, stellt sich die Frage, was „Löschen" eigentlich genau bedeutet. Eine Definition, was Löschen bedeutet, enthält die DSGVO nicht. Ein Mitarbeiter einer deutschen Datenschutzaufsichtsbehörde formulierte es kernig einmal so: Löschen heißt Löschen (vgl. zur Auffassung der dänischen Datenschutzaufsichtsbehörde und zur Nachweispflicht auch oben Fall 22). „Sperren" ist hingegen etwas anderes, nämlich die sehr enge Begrenzung des Kreises der Personen, die auf ein personenbezogenes Datum zugreifen dürfen, aufgrund der engen Zweckbindung (z. B. Aufbewahrung zu steuerlichen Zwecken, vgl. oben Fall 21). Mit anderen Worten: „Sperren" ist im Wesentlichen eine Frage des (verengten) Berechtigungskonzepts und dessen Durchsetzung mit technisch-organisatorischen Maßnahmen. Wo gelöscht werden muss, reicht die Sperrung nicht aus.

Umgekehrt aber ist das Löschen vom „Vernichten" zu unterscheiden, denn die DSGVO nennt beides nebeneinander als Verarbeitungshandlungen, weshalb beide Begriffe wohl etwas Unterschiedliches bedeuten müssen. So kann Löschen auch durch Anonymisieren erreicht werden, ohne dass die Daten tatsächlich (vollständig) vernichtet werden (s. unten Fall 32). Löschen ist demnach – im Unterschied zur Vernichtung – das „Unkenntlichmachen" der Daten. Wo gelöscht werden muss, muss also nicht unbedingt vernichtet werden.

Dies wiederum wirft in der IT-Welt die Frage auf, ob das Löschen von Metadaten ein Löschen der Daten selbst sein bzw. ersetzen kann. Es gibt juristische Kommentare, nach denen *„die Löschung von Verknüpfungen oder Codierungen, die zur Wahrnehmung der Information erforderlich sind"*, ausreichend ist. Die Beantwortung dieser Frage ist für viele IT-Verantwortliche essentiell. Entscheidend ist der Grad an Aufwand, der notwendig ist, um die Information ohne Metadaten wiederherzustellen. Ist dies mit einfachen Tools möglich, wie etwa bei Dateien, die nur in einem Datenträgerverzeichnis (*„file allocation table"*) gelöscht wurden, stellt das Löschen dieser Zuordnungs- bzw. Metadaten sicherlich kein Löschen dar. Anders könnte es sein, wenn in komplexen Datenbankstrukturen (wie einem SAP-System) sämtliche Referenzen auf einzelne Datenbankinhalte gelöscht werden, sodass diese nur durch eine aufwändige Analyse des Datenbankinhalts auf „Rohdatenebene" wiederherstellbar wären. Sobald aber Werkzeuge verfügbar werden, die eine derartige Analyse vereinfachen, könnten bisher als gelöscht geglaubte Daten als „Zombies" wieder auferstehen, sprich doch nicht gelöscht worden sein. Je verbreiteter eine Software ist, desto größer das Risiko, dass derartige „Undelete-Werkzeuge" entwickelt werden.

Der Europäische Datenschutzausschuss hat in seinen Empfehlungen vom November 2019 zum Thema *„privacy by design/by default“* sinngemäß „Beobachtungspflichten hinsichtlich der allgemeinen technischen Entwicklungen“ statuiert (s. unten Fall 32). Es gibt also einiges zu tun für die Verantwortlichen, die „nur“ Verknüpfungen löschen.

- Müssen berichtigte (vormalige) Daten gelöscht werden?

Eine interessante Frage zum Abschluss ist, ob bei einer Berichtigung von Daten die ursprünglichen Daten (unaufgefordert) gelöscht werden müssen. Hier ist auf zwei Gerichtsentscheidungen zu verweisen, die sich u. a. mit dieser Fragestellung beschäftigen. Das Oberverwaltungsgericht Hamburg hat im Mai 2019 entschieden, dass eine Änderung des Vornamens eines Mitarbeiters infolge einer Geschlechtsumwandlung nicht dazu führt, dass der alte Vorname zu löschen ist. Denn dieser ist nicht historisch falsch gewesen, sondern wurde – wie der Jurist sagt – nur mit Wirkung für die Zukunft geändert (*„ex nunc“*). Das Oberverwaltungsgericht Hamburg führt aus:

„Die Beklagte hält ihre Personalakten bewusst auf dem Stand, der zum jeweiligen Zeitpunkt richtig war, um ein möglichst lückenloses Bild der Entstehung und Entwicklung des Dienstverhältnisses als historischem Geschehensablauf dokumentieren zu können, so dass sie die Daten auch nicht dem neuesten Stand anpassen muss; eine solche Anpassung, die aus den Akten nicht erkennbar wäre, könnte vielmehr umgekehrt gegen den Grundsatz der Datenrichtigkeit verstoßen“.

Was hier nicht erörtert wird, ist die Frage, wozu der vormalige Vorname überhaupt noch benötigt wird. Im Kontext des § 26 BDSG wäre also zu fragen, ob die Verarbeitung des vormaligen Vornamens noch *„zur Durchführung eines Beschäftigungsverhältnisses erforderlich“* ist. Wäre dies nicht der Fall, wäre kaum ersichtlich, weshalb der alte Datenstand nicht gelöscht werden müsste.

Daneben hat das österreichische Landesgericht Feldkirch in einer in Fachkreisen weit beachteten Entscheidung gegen die österreichische Post – weit beachtet, weil dort ein Ersatz immateriellen Schadens (in Höhe von EUR 800) zugesprochen wurde – die Fortspeicherung vormaliger Adressen durch ein Telekommunikationsunternehmen für rechtmäßig erachtet. Die historischen Adressen wurden im Rahmen eines gesonderten Services gespeichert, der wie folgt umschrieben wird:

„Die beklagte Partei bietet Unternehmen das sogenannte „ADRESS-CHECK-Service“ an. Dieses ermöglicht Unternehmen, ihre Kundendaten mit den von der beklagten Partei gespeicherten Umzugsdaten abzugleichen und dadurch die neue Adresse verzogener Kunden

zu erfahren. So können Unternehmen mit ihren verzogenen Kunden ohne langwierige und teure Nachforschungen in Kontakt bleiben. Weil umziehende Personen häufig nicht allen Unternehmen, mit denen sie in Kontakt sind oder waren, ihre neue Adresse mitteilen, kommt es nach einem Umzug oft auch noch nach langer Zeit zu Postsendungen an eine alte, nicht mehr aktuelle Adresse. Um bei möglichst vielen Unternehmen die neue Adresse bekanntgeben zu können und nicht zustellbare Sendungen zu vermeiden, speichert die beklagte Partei frühere Wohnadressen von Personen, die der Datenverwendung für Marketingzwecke Dritter nicht widersprochen haben, über mehrere Jahre".

Auf der Basis welcher Legitimationsgrundlage die historischen Adressdaten verarbeitet wurden, lässt das Urteil offen, führt aber allgemein hierzu aus:

„Im Zusammenhang mit dem von der beklagten Partei angebotenen „ADRESS-CHECK-Service" erscheint es angemessen und legitim, auch mehrere frühere Adressen des Klägers in Verbindung mit dem Vermerk „verzogen" über mehrere Jahre zu speichern. [...] Zumal die früheren Adressen des Klägers im Speichersystem der beklagten Partei ohnehin mit dem Vermerk „verzogen" versehen sind, ist auch ein Verstoß gegen den Grundsatz der Datenrichtigkeit nach Art. 5 Abs. 1 lit. d DSGVO nicht erkennbar."

Auch wird die weitere Speicherung der veralteten Informationen trotz zwischenzeitlicher Berichtigung als rechtmäßig angesehen, um den Betroffenen auch nach einem Umzug mit Werbung „verfolgen" zu können.

Fall 29:
Im Gestrüpp der Interessenabwägung

Praktischer Fall: Die Finanzberatung Maier GmbH berät verschiedene Kunden, sowohl Unternehmen als auch Privatpersonen, über Möglichkeiten der Finanzanlage. Dies geschieht in unterschiedlichen Themenbereichen und Zielgruppen. Die Maier GmbH möchte sowohl ihren Kunden als auch interessierten Dritten Marketing-Materialien zukommen lassen, um so mit diesen in Kontakt zu bleiben bzw. sich wieder in Erinnerung zu rufen. Dies umfasst „Newsletter" in schriftlicher und E-Mail-Form, Einladungen zu Veranstaltungen, Weihnachtskarten etc. Interessierte Dritte sind insbesondere Personen, deren Kontaktdaten die Mitarbeiter der Maier GmbH bei Veranstaltungen, durch Vermittlung seitens Geschäftspartnern oder anlässlich spontaner Kontaktaufnahme durch die Dritten „aufsammeln". Dabei werden von den Mitarbeiter der Maier GmbH teilweise, etwa wenn ihnen gegenüber nur ein Nachname und ein Unternehmensname eines Ansprechpartners genannt wurden, auch Informationen aus dem Impressum der betroffenen Unternehmenswebsite verwendet. Intern versieht die Maier GmbH die Daten dann mit „Tags", d. h. für welche (Finanzierungs-)Felder sich welche Kunden und Dritte interessieren, und generiert so Interessengruppen bzw. relevante Teilmengen (Mailing-Listen). Welche Marketing-Materialien welchen Teilmengen zugesandt werden, wird jeweils von Fall zu Fall entschieden. Teils werden auch Marketing-„Formate" ausprobiert, z. B. die Ansprache ausgewählter Personen für ein ansprechendes Abendessen mit Kurzvortrag, eine Unternehmensjubiläumsfeier oder die Zusendung von kleinen „Gadgets" wie Briefbeschwerer mit Unternehmensaufdruck etc. Die Maier GmbH versieht daher vorsorglich jede Außenkommunikation (Verträge mit Kunden und Dritten, E-Mail-Verkehr etc.) mit dem Hinweis, dass die personenbezogenen Daten des Adressaten „auch" zu „Zwecken des Direktmarketings" verwendet werden, und verweist jeweils auf eine entsprechende Internetseite, welche die entsprechenden Pflichtinformationen enthält.

Die vorhergehenden Fälle zu Themen des Direktmarketings (Fälle 1, 8, 17, 20 und 26) behandeln bereits einige Facetten dieser Fallgestaltung. Hier soll es vorrangig um die Frage der Interessenabwägung selbst gehen. Dass das Interesse an „Direktmarketing" ein datenschutzrechtlich legitimes Interesse ist, ergibt sich aus der DSGVO selbst, wobei auch schon hier die Frage der Reichweite des Begriffs „Direktmarketing" offen ist (Bestandskunden vs. Neukunden, s. oben Fall 8). Welches Interesse eines Betroffenen dem im Rahmen einer Abwägung entgegenstehen kann, ist auch nicht ganz so klar. Der Wettbewerbsrechtler würde sagen, dass (außerhalb des Bereichs der Einwilligung) im Grundsatz jede „Belästigung" des Betroffenen mit Werbung unzumutbar ist, soweit das Gesetz diese nicht ausnahmsweise erlaubt. So wurde zum Beispiel aus wettbewerbsrechtlicher Sicht – und auf klarer gesetzlicher

Grundlage – geurteilt, dass ein Online-Händler, der ein breites Warenspektrum vertreibt, keinen „10%-Rabattgutschein auf Alles“ an einen Kunden senden darf, der zuvor dort ein Notebook erworben hat. Der Gutschein – der natürlich eine Werbung darstellt – darf sich nicht auf Waschmaschinen (und was der Händler sonst noch alles im Portfolio hat) beziehen, sondern nur auf Notebooks und „ähnliche“ Produkte (vgl. auch oben Fall 17). Man mag das für seltsam halten, weil die „Belästigung“ hier erlaubt gewesen wäre, wenn der Gutschein nur „10% auf Notebooks“ gelautet hätte. Warum aber sollte der Kunde so schnell schon einen zweiten, ähnlichen Notebook erwerben wollen? Und warum darf nicht für Zubehör (z. B. eine Computermaus) geworben werden, welches dem Notebook leider nicht „ähnlich“ ist? Zumindest aber ist das Wettbewerbsrecht in diesem Punkt sprachlich klar abgefasst und macht es dem Rechtsanwender geradezu einfach (was viele Juristen nicht freuen dürfte). In der DSGVO hingegen fehlen konkrete Anhaltspunkte dafür, wann eine unzumutbare Belästigung vorliegt bzw. welche Interessen des Werbungsadressaten in welcher Gewichtung zu berücksichtigen sind.

- Folge dem Wettbewerbsrecht?

Das leitet auf die entsprechende Logik der Interessenabwägung im Rahmen der DSGVO über. Schon das Wort „Interessenabwägung“ selbst indiziert ja, dass man es so oder so sehen kann, je nachdem, welchem Interesse man nun größeres Gewicht einräumt. Und als sei die Identifikation der beiderseitigen legitimen Interessen und die Abwägung dieser Interessen noch nicht genug, wird in den Erwägungsgründen der DSGVO zusätzlich vorgeschrieben, dass bei der Interessenabwägung „die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen“ sind. Mit anderen Worten: Wenn ein vernünftiger Betroffener sagen würde „wer X macht, muss mit Y rechnen“, dann wäre das ein Indiz, das Y datenschutzrechtlich erlaubt ist. Und würde nicht jemand, der ein Notebook kauft, auch Werbung für eine Computermaus erwarten?

Wettbewerbsrechtlich wird hier nach dem Medium unterschieden – also ob die Ansprache per Post, E-Mail oder Telefon erfolgt –, welches aber datenschutzrechtlich irrelevant ist. Die Datenschutzkonferenz begründet mithilfe des skizzierten „Erwartungsgrundsatzes“ ihre Aussage in ihrer „Orientierungshilfe“ zum Thema Direktwerbung vom November 2018, es sei datenschutzrechtlich zulässig, wenn im Nachgang zu einer Bestellung postalisch (!) ein Werbekatalog oder ein Werbeschreiben zum Kauf (beliebiger) weiterer Produkte des Verantwortlichen zugesendet wird. Damit stellt hier die Datenschutzkonferenz auf ein bestimmtes Medium ab (was für das Datenschutzrecht untypisch ist) und verfolgt inhaltlich, aus wettbewerbsrechtlicher Perspektive, eine Mittellösung zwischen postalischen Sendungen (bei denen alles erlaubt ist, solange der Angesprochene nicht explizit widersprochen hat) und

E-Mail-Werbung (bei der nur für ähnliche Waren bzw. Dienstleistungen geworben werden darf, s. o.). Den Zweck des Vertragsverhältnisses (Notebook-Kauf und dessen Abwicklung), der datenschutzrechtlich gerade die (ursprüngliche) Zweckbindung kennzeichnet (s. oben Fall 17), überschreitet die Datenschutzkonferenz dabei aber jedenfalls deutlich. Ist also nun die enge datenschutzrechtliche Zweckbindung an den Notebook-Kaufvertrag Makulatur?

Eher nicht. Denn die Datenschutzbehörden bevorzugen letztlich in der Sache die „Zwei-Säulen-Lösung" über eine Interessenabwägung zu Direktmarketingzwecken (s. oben Fall 17), die als datenschutzrechtliche Legitimationsgrundlage neben das Kaufvertragsverhältnis tritt. Der ursprüngliche (Kauf-)Vertrag als solcher spielt daher auch in der nachfolgenden Argumentation der Datenschutzbehörden zur Interessenabwägung und zur Erwartungshaltung des Betroffenen keine Rolle mehr. Auch weitere Beispiele der Datenschutzbehörden zu einer zulässigen Direktmarketing-Interessenabwägung stehen immer noch im Zusammenhang mit einem bestehenden (Preisausschreiben) oder angestrebten (Katalog- und Prospektanforderungen) Vertrag bzw. vertragsähnlichen Verhältnis, ohne dass dort die Frage der Relevanz dieser Beziehung für die Interessenabwägung thematisiert wird. Dabei kann man einem bestehenden Vertragsverhältnis für die Frage des (zusätzlichen) Direktmarketings durchaus zwei gegensätzliche Bedeutungen zuschreiben: Einerseits ist der Vertrag der eigentliche Grund dafür, dass das Unternehmen überhaupt über die personenbezogenen Daten des Kunden verfügt. Man könnte also argumentieren, dass Werbung „auf der Basis der Vertragsdaten" nur eng betrieben werden darf, weil der Betroffene, der den Vertrag schließen möchte, gezwungen ist, dafür bestimmte Daten an den Verantwortlichen zu geben. So sieht es ja im Übrigen auch das Wettbewerbsrecht im Bereich der elektronischen Medien, worauf wir gleich noch einmal zurückkommen werden. Andererseits ist aber die bestehende vertragliche Beziehung immerhin ein veritabler Anknüpfungspunkt, oder anders ausgedrückt: Wenn es nun gar keine Vertragsbeziehung zwischen Verantwortlichem und Betroffenem gäbe, würde dies die Interessenabwägung hinsichtlich Direktmarketing anders ausfallen lassen als beim Bestehen einer vertraglichen Verbindung? Man könnte argumentieren, dass ohne Vertrag noch weniger geworben werden darf.

Nun dürfte allerdings die Bewerbung von Adressen mit postalischen Sendungen – innerhalb oder außerhalb bestehender Vertragsbeziehungen – bei Weitem nicht mehr den Schwerpunkt der Werbetätigkeit darstellen. Für die entscheidende Frage, was bei elektronischer Kommunikation gilt, kann nur auf den von der Datenschutzkonferenz im Rahmen der Interessenabwägung allgemein postulierten Grundsatz „Datenschutzrecht folgt Wettbewerbsrecht" verwiesen werden – was wettbewerbsrechtlich verboten ist, darf also datenschutz-

rechtlich nicht das Ergebnis einer Interessenabwägung sein. Diese „Übertragung" der wettbewerbsrechtlichen Eingrenzung auf „ähnliche Waren und Dienstleistungen" im Bereich der E-Mail würde zwar den Zweckzusammenhang mit dem ursprünglich bestehenden Vertrag stärker gewichten. Aber der sich dadurch ergebende Unterschied zur Auffassung der Datenschutzbehörden bezüglich postalischer Werbeansprachen (der gerade nicht dem Wettbewerbsrecht entspricht, s. oben) kann damit aus spezifisch datenschutzrechtlicher Perspektive nur schlecht erklärt werden: Die Erwägungsgründe der DSGVO sehen ausdrücklich „Direktwerbung" als legitimen Zweck an und gerade nicht „Direktmarketing gegenüber Bestandskunden im Hinblick auf ähnliche Waren und Dienstleistungen". Und eine Unterscheidung nach dem Übermittlungsmedium findet sich hier schon gar nicht.

In einer Entscheidung der österreichischen Datenschutzbehörde vom März 2019 wurde der pauschale Grundsatz „Datenschutzrecht folgt Wettbewerbsrecht" im Zusammenhang mit einer „Re-Opt-In-Kampagne" bekräftigt. Der Betroffene hatte 2014 an einer Marketing-Veranstaltung teilgenommen und dabei seine Kontaktdaten angegeben. Der Verantwortliche hatte wesentlich später, um den Zeit des Inkrafttretens der DSGVO, per E-Mail gefragt, ob der Betroffene weiterhin „in Kontakt bleiben" wolle, und der Betroffene hatte darauf nicht geantwortet, war aber kurz darauf wieder mit Werbe-E-Mails desselben Verantwortlichen konfrontiert worden. Nach (deutschem und österreichischem) Wettbewerbsrecht war letzteres unzulässig (eine Einwilligung lag nicht vor), und die Datenschutzbehörde entschied, dass eine wettbewerbswidrige Werbung auch eine DSGVO-widrige Werbung sei. Die Unzulässigkeit einer E-Mail-Werbung ohne Einwilligung ergebe sich aus der ePrivacy-Richtlinie 2002 (von der österreichischen Datenschutzbehörde „e-Datenschutz-Richtlinie" genannt) und „daher" könne die Datenverarbeitung auch nicht unter der DSGVO alternativ auf eine Interessenabwägung gestützt werden. Die Begründung für diese Parallelität beruht auf Art. 95 DSGVO, wonach die DSGVO den Verantwortlichen „keine zusätzlichen Pflichten" im Verhältnis zur ePrivacy-Verordnung auferlegt. Der Betroffene durfte deshalb diese Rechtsverletzung auch mit einer „Datenschutzbeschwerde" rügen. Aber selbst wenn eine alternative Legitimationsgrundlage unter der DSGVO denkbar gewesen wäre: Vielleicht wäre das Interesse des Verantwortlichen an Direktmarketing ohnehin zwischenzeitlich verblasst gewesen (vgl. o. Fall 8)?

➢ Interessenabwägung und „induzierte" Erwartungshaltung

Unabhängig von der (offenen) Frage, wie Vertrag und Direktmarketing wechselwirken und wie bestimmend das im Bereich der E-Mail auf der ePrivacy-Richtlinie basierende Wettbewerbsrecht für die datenschutzrechtliche Einordnung ist, bedarf die – separate – zweite Säule des Direktmarketings aber, wie jede andere Interessenabwägung auch, jedenfalls materiell

einer entsprechenden Interessenabwägung und formal einer entsprechenden Aufklärung des Betroffenen (Pflichthinweise), die diese Interessenabwägung „nach außen“ spiegelt. Der in den Erwägungsgründen der DSGVO verankerte „Erwartungsgrundsatz“ (s. o.) vermischt nun diese beiden Sphären: Je besser der Verantwortliche über die Reichweite der beabsichtigten Datenverarbeitung formal aufklärt, desto mehr darf er auch materiell tun. Anders ausgedrückt macht eine gute Aufklärung mehr möglich. Die Datenschutzbehörden formulieren das so:

„Informiert der Verantwortliche transparent und umfassend über eine vorgesehene Verarbeitung von Daten für Zwecke der Direktwerbung, geht die Erwartung der betroffenen Personen in aller Regel auch dahin, dass ihre Kundendaten entsprechend genutzt werden.“

Dieser kluge Satz gibt die Selbstverständlichkeit wieder, dass der Verantwortliche die „vernünftigen Erwartungen der betroffenen Person“ selbst steuern kann: Wenn man jemandem ankündigt, dass man ihn demnächst beleidigen wird, ist die Erwartung der Beleidigung eine vernünftige Erwartung. Aber dadurch wird die Beleidigung eigentlich nicht zulässiger. Ist das nun im Datenschutzrecht anders? Zumindest muss es eine Grenze für diese Regel geben, um zu verhindern, dass „irgendetwas“ angekündigt wird, was nach dieser Logik dann auch (automatisch) zulässig wäre. Deshalb formuliert die Datenschutzkonferenz folgerichtig weiter:

„Allerdings kann durch Transparenz der gesetzliche Abwägungstatbestand nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO nicht beliebig erweitert werden, da die Erwartungen an dem objektiven Maßstab der Vernunft gemessen werden müssen.“

Wenn der Gesetzgeber also keine konkreten Vorgaben für die Interessenabwägung zu Direktmarketingzwecken erlässt, muss anstelle des Gesetzgebers der „objektive Maßstab der Vernunft“ zur Anwendung kommen. Wie immer in solchen Situationen wird ein methodischer Standardtrick der Juristen verwendet: Es wird einfach ein neuer Begriff aus dem Hut gezaubert, um den ursprünglichen Begriff zu definieren. Die Unklarheit der Interessenabwägung beim Thema Direktmarketing wird nun durch die Unsicherheit ersetzt, wo die Grenze des „objektiven Maßstabs der Vernunft“ bei der Beeinflussung der Interessenabwägung durch transparente Aufklärung liegt.

- Medienbruch bei Pflichthinweisen

Nach dieser im Ergebnis wenig befriedigenden Einleitung zur Struktur der Interessenabwägung stellen sich nun im Ausgangsfall verschiedene Fragen. Erstens geht es im Rahmen der formalen Aufklärung (Pflichthinweise) um das Thema „Medienbruch“: Ein wesentlicher Teil

der Pflichthinweise an den Betroffenen ist nicht in der „Primärkommunikation“ (E-Mail etc.) enthalten, sondern auf einer Website, auf die verwiesen wird. Im Grundsatz soll das zulässig sein – auch die Datenschutzkonferenz spricht von der Möglichkeit eines Weblinks –, nur: Was genau nun wo stehen muss bzw. darf, ist unklar. Die Datenschutzkonferenz führt derart viele Informationen auf, die bereits in der „Primärkommunikation“ enthalten sein sollen, dass man sich fragt, was dann eigentlich überhaupt noch auf die Website ausgelagert werden darf. Vor diesem Hintergrund ist auch der weitere Hinweis der Datenschutzkonferenz, dass „stets der Informationsbedarf im Einzelfall entscheidend ist“, wenig hilfreich. Das bayerische Landesamt für Datenschutzaufsicht sieht diese „erste Stufe“ in seinem Tätigkeitsbericht 2017/2018 wohl etwas gelassener:

„Auf der ersten Stufe bzw. im ersten Schritt müssen immer die Informationen zur Identität des Verantwortlichen und zu den Zwecken der Verarbeitung gegeben werden, soweit diese Informationen nicht ohnehin schon wegen der Art des Kontakts mit der betroffenen Person offenkundig sind (z. B. bei deren Anruf zu einer Terminvereinbarung mit dem Friseur oder Steuerberater). Je nach Art des Kontakts mit der betroffenen Person ist ergänzend noch auf das Bestehen der Betroffenenrechte hinzuweisen, z. B. in Werbeschreiben.“

Wie sich der Europäische Datenschutzausschuss eine „*layering*“-Technik bei Pflichthinweisen vorstellt, wurde bereits oben in Fall 26 dargestellt.

➢ Direktmarketing mit der Bratpfanne

Zweitens wird im Ausgangsfall, den praktischen Notwendigkeiten folgend, pauschal gegenüber jedem Kommunikationspartner Direktmarketing angekündigt, aber in vielen Fällen kommt dies gar nicht zur Anwendung (s. auch oben Fall 26). Wenn sich etwa ein Bewerber bei der Maier GmbH bewirbt oder der Mineralwasserlieferant der Maier GmbH per E-Mail fragt, ob er für die nächste Lieferung auch am Dienstagnachmittag kommen darf, ist der Zusatz in der Antwort-E-Mail der Maier GmbH nicht „ernst gemeint“, weil die Person – aus der Perspektive der Maier GmbH – nicht zu einer relevanten Zielgruppe für Direktmarketing zählt. Ist das nun unschädlich, weil man gegenüber diesen Personen ja auch Direktmarketing betreiben dürfte (was zu beweisen wäre)? Oder ist die Frage der Interessenabwägung überhaupt nur dann bedeutsam, wenn später auch wirklich Direktmarketing gegenüber der Person betrieben wird? Oder muss nun doch das gesamte Personal der Maier GmbH dazu geschult werden, wann ein solcher Zusatz einer E-Mail manuell hinzugefügt werden muss? Und was, wenn der Zusatz dann einmal irrtümlich vergessen wird, aber diese Person später Direktmarketing-Informationen erhält? Oder wenn der Zusatz einmal irrtümlich hinzugesetzt wird, aber diese Person nie Direktmarketing-Informationen erhalten würde?

- Ist „Direktmarketing“ granular genug?

Drittens stellt sich die Frage, inwieweit im Rahmen der Pflichthinweise, die ja auch die Erwartungshaltung des Betroffenen prägen, pauschal „Direktmarketing“ als Zweck angegeben werden kann. Die meisten Datenschützer werden sagen, dass dies konkretisiert werden muss, auch wenn sie selbst nicht weiter werden konkretisieren können, was das konkret bedeutet. In Empfehlungen vom April 2019 verwies der Europäische Datenschutzausschuss auf die bereits 2013 von der Art.-29-Datenschutzgruppe geäußerten Vorgaben für die Konkretisierung des Verarbeitungszwecks:

“The purpose of the collection must be clearly and specifically identified: it must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied. For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will - without more detail - usually not meet the criteria of being ‘specific’.”

In die gleiche Richtung führt das österreichische Bundesverwaltungsgericht in einer Entscheidung vom Dezember 2018 aus:

„Zweckangaben wie "Verbesserung der Benutzerfreundlichkeit", "Marketingzwecke", "Zwecke der IT-Sicherheit", "künftige Forschung" sind zu allgemein und erfüllen nicht das Kriterium der hinreichenden Bestimmtheit. Als Faustregel ist anzuraten, einen Zweck idR in mehr als drei Worten anzugeben, ohne allerdings in ausufernde, unübersichtliche und komplizierte Formulierungen zu verfallen. Praktische Beispiele zur Festlegung der Verarbeitungszwecke finden sich in Anhang 3 des WP203 der Artikel-29-Datenschutzgruppe.

Daraus geht hervor, dass nicht nur die Subsumption von - gegenständlich - Datenverwendungen für Marketing- und Werbezwecke unter "damit verbundene Serviceleistungen" nicht ausreichend konkret und transparent ist, sondern auch eine Auskunft nur betreffend "Marketing- und Werbezwecke" nicht genügen wird. Vor dem Hintergrund der Datenschutzerklärung der Beschwerdegegnerin wäre zumindest der Zweck der Direktwerbung zu beauskunften gewesen.“

Demgegenüber enthält das „Muster für gute Auskunft nach Art. 15 DS-GVO“ des bayerischen Landesamts für Datenschutzaufsicht als Muster-Angabe unter der Überschrift „Verarbeitungszwecke“ die Angabe: *„Wir nutzen Ihre oben stehenden Daten ausschließlich zum*

Zwecke der Direktwerbung". Darf das hier laxer gehandhabt werden als bei der Definition des Verarbeitungszwecks und den entsprechenden Pflichthinweisen? Dieselbe Behörde sieht zum Beispiel keinen (Zweck-)Unterscheid zwischen werblicher Ansprache im engeren Sinne (Anbieten von Produkten und Dienstleistungen) und der Versendung von Weihnachts-, Neujahrs- und sonstigen Glückwunschkarten, sodass die Pflichtinformationen auch einheitlich „genutzt" werden können:

„Nach dem von der Rechtsprechung sehr weit definierten Begriff der Werbung sind Weihnachts- und Neujahrswunschkarten von Firmen an ihre Geschäftspartner als werbliche Maßnahmen anzusehen, die dem Aufbau und der Pflege von Geschäftsbeziehungen dienen und damit das Geschäft fördern sollen. Allerdings steht das Datenschutzrecht mit der Regelung in Art. 6 Abs. 1 Satz 1 Buchstabe f DSGVO der Verwendung von Postadressdaten für die Zusendung von Weihnachts-, Neujahrs- und sonstigen Glückwunschkarten durch Firmen regelmäßig nicht entgegen, solange eventuelle Werbewidersprüche beachtet werden. Wenn bei bestehenden Geschäfts- oder Kundenbeziehungen die gesetzlich vorgesehenen Informationen nach Art. 13 und Art. 21 Abs. 4 DS-GVO schon im Laufe des Jahres erfolgt sind, können diese Informationen bei den Weihnachts- oder Neujahrsgrüßen unterbleiben (wo sie ohnehin nur störend wirken würden)."

Beim Parallelfall der „informierten" Einwilligung fordert die Datenschutzkonferenz bekanntlich (s. oben Fall 8), dass *„die Produkte oder Dienstleistungen, für die geworben werden soll"*, dem Einwilligenden bekannt sein müssen. Was heißt das nun bei einem breiten Portfolio an Waren oder Dienstleistungen, welches auch Änderungen unterworfen sein kann, und wie konkret müssen die Produkt- oder Dienstleistungsgruppen bezeichnet werden? Reicht es aus, wenn man „Newsletter" schreibt, weil das im Zweifel die Produkte und Dienstleistungen betreffen wird, die das Unternehmen eben von Zeit zu Zeit anbietet? Ähnliche Fragen stellen sich auch in Bezug auf das Werbeformat. Muss ein Newsletter, der vier Mal im Jahr erscheint, als „regelmäßig" angegeben werden – und was ist, wenn er nur „in loser Folge" erscheint, vielleicht ein Jahr lang gar nicht? Und wenn man verlangen würde, dass hier zumindest das „Werbeformat" genannt werden muss, schließt dies dann die Kontaktaufnahme für innovative Werbeformate, die ad hoc entwickelt werden, aus? Für wettbewerbsrechtliche Einwilligungserklärungen und verschiedene „Werbekanäle" hat der Bundesgerichtshof immerhin im Februar 2018 geurteilt, dass der Satz *„Ich möchte künftig über neue Angebote und Services der T-GmbH per E-Mail, Telefon, SMS oder MMS persönlich informiert und beraten werden"* zulässig ist: Eine eigene Einwilligungserklärung für jeden „Werbekanal" ist nicht erforderlich.

➢ Targets aus öffentlich zugänglichen Quellen

Viertens werden im Ausgangsfall auch öffentlich zugängliche Quellen, hier in Gestalt des Impressums, zur Datengewinnung herangezogen. Die Datenschutzkonferenz will dies mit einer auf den ersten Blick einleuchtenden Argumentation verbieten: Die Daten im Impressum – etwa die Angabe des vollen Namens des Geschäftsführers – müssen vom Websitebetreiber aufgrund zwingender gesetzlicher Vorschriften (Impressumspflicht) bereitgestellt werden. Da das Unternehmen keine andere Wahl hat, als diesen Pflichten zu genügen, kann nicht davon ausgegangen werden, dass diese Daten für Werbezwecke Dritter gegenüber den im Impressum genannten Personen bereitgestellt werden sollten. Daher würde hier das Interesse an Direktwerbung, nicht das Interesse, nicht mit Werbung belästigt zu werden, überwiegen – von einer „Einwilligung" durch das Einstellen auf die eigene Website ganz zu schweigen. Ähnlich hat auch die österreichische Datenschutzbehörde im Oktober 2018 entschieden, dass eine auf einer Website veröffentlichte Telefonnummer einer „Beratungshotline" für bedürftige Personen zweckwidrig für Werbemaßnahmen verarbeitet wird, wenn sie für Direktmarketing-Zwecke (Cold-Calling zur Produktbewerbung) genutzt wird.

Dabei fällt allerdings schon unter den Tisch (s. oben Fall 20), dass sich die dann folgende Werbung eigentlich gar nicht an die angesprochene Person „persönlich" richtet, sondern an das Unternehmen, das eben nun einmal ausschließlich durch natürliche Personen repräsentiert wird und werden kann. Immerhin handelt es sich bei den Impressumsangaben auf Unternehmenswebsites nicht um Informationen der Privatsphäre, sondern um unternehmensbezogene Kontaktdaten. Hinzu kommt, dass nach dem von der Datenschutzkonferenz sonst bisweilen als „Vorbild" gepriesenen Wettbewerbsrecht von einer stillschweigenden Einwilligung eines Unternehmens in die unaufgeforderte telefonische Kontaktaufnahme zu Werbezwecken ausgegangen werden kann, wenn diese Kontaktaufnahme zur Zwecken erfolgt, die mit dem Geschäftsgegenstand bzw. den Bedürfnissen des Zielunternehmens im Zusammenhang stehen. Mit anderen Worten: Ein Unternehmen, das Maschinen verkauft, darf man auch ohne Aufforderung anrufen und fragen, ob es am Einkauf von Stahlteilen interessiert ist – nicht aber an neuen Kollektionsstoffen. Im B2B-Bereich wird demnach unterstellt, dass ein Unternehmen eine gewisse (telefonische) „Belästigung" aushalten muss, weil es werblich am Markt auftritt. Die dazu ergangene Rechtsprechung wird sogar von der Datenschutzkonferenz selbst, wenn auch in anderem Zusammenhang, zitiert. Diese wettbewerbsrechtliche Erleichterung der telefonischen Kontaktaufnahme setzt sich allerdings nicht fort, wenn es um die – in der Praxis wichtige – Ansprache per E-Mail geht. Das ist auch der Grund, weshalb in der Praxis vermutlich meist das Wettbewerbsrecht strenger sein wird; wir werden darauf in Kürze noch zurückkommen.

Dass die Rechtsprechung in diesem Bereich noch alles andere als „gefestigt“ ist, kann aber einem Urteil des Verwaltungsgerichts Saarland vom März 2018 entnommen werden, das vom Oberverwaltungsgericht Saarland im September 2019 bestätigt wurde. Hier hatte ein Unternehmen, das Edelmetallreste von Zahnarztpraxen und Dentallaboren ankauft, aus öffentlich zugänglichen Quellen („Gelbe Seiten“) die Anschrift und Telefonnummer von Praxen ermittelt und dort telefonisch in Erfahrung gebracht, ob Interesse an einem Verkauf von Edelmetallresten besteht. Das Verwaltungsgericht Saarland hielt diese Praxis unter dem damaligen BDSG (und UWG) nicht für zulässig. Es sei zu berücksichtigen, dass der Verkauf von Edelmetallresten nicht zum *„eigentlichen Tätigkeitsbereich eines Zahnarztes“* gehöre, sondern *„sich Zahnärzten hier allenfalls die Möglichkeit einer zusätzlichen Einnahmequelle“* biete. Die Veröffentlichung der Telefonnummer der Praxis diene in erster Linie dazu, dass Patienten Kontakt aufnehmen können. Werbeanrufe könnten den Praxisbetrieb stören: Wenn nun jeder Vertreiber von Leistungen, die Zahnärzte „irgendwie“ mal benötigen könnten, anrufe, dann könne die Praxis nicht mehr vernünftig arbeiten. Es sei auch nicht ersichtlich, dass dieses Verhalten unter der (aus damaliger Sicht: künftigen) DSGVO (Art. 6 Abs. 1 S. 1 lit. f DSGVO) gerechtfertigt sein wird: *„Es bliebe zunächst abzuwarten, wie die Vorschrift von Rechtsprechung und Literatur ausgelegt werde“*. Man sieht also, wie „fein“ hier die Linien gezeichnet werden.

Auch vom Betroffenen freiwillig (also ohne Rechtspflicht wie beim Impressum) selbst ins Internet (oder in die „Gelben Seiten“) gestellte Informationen sind demnach kein Garant dafür, dass eine Interessenabwägung zulasten des Betroffenen ausgeht. Es ist vielmehr der (offensichtliche) Zweck, zu dem die Daten veröffentlicht wurden, zu berücksichtigen. Dies würde, wenn man neben einer Ausnahme nach Art. 9 DSGVO die Notwendigkeit einer selbstständigen Legitimationsgrundlage nach Art. 6 DSGVO annimmt (dazu oben Fall 2), auch für personenbezogene Daten besonderer Kategorien gelten: Diese dürfen zwar nach Art. 9 Abs. 2 lit. e) DSGVO grundsätzlich (und gleich zu welchem Zweck) verarbeitet werden, wenn sich *„die Verarbeitung auf personenbezogene Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat“*. Aber wenn zusätzlich auch eine Legitimationsgrundlage im Sinne des Art. 6 DSGVO notwendig ist, etwa in Form einer Interessenabwägung, kann auch hier wieder der Veröffentlichungszweck herangezogen werden müssen. Die Existenz der Regelung in Art. 9 Abs. 2 lit. e) DSGVO heißt also nicht, dass auch für „gewöhnliche“ Daten nicht nach dem Veröffentlichungszweck differenziert werden muss.

- Bildung von Interessengruppen

Fünftens stellt sich im Ausgangsfall die Frage, ob die Selektion der Kontakte in Interessengruppen datenschutzrechtlich zulässig ist. Die Datenschutzkonferenz nimmt das an, jedoch

nur unter der Voraussetzung, dass sich aus der Selektion anhand von Selektionskriterien kein „zusätzlicher Erkenntnisgewinn“ ergibt. Damit soll eine Abgrenzung zu dem – aus Sicht der Datenschutzkonferenz im Rahmen der Interessenabwägung als Legitimationsgrundlage nicht mehr zulässigen – Profiling gezogen werden. Nun ist aber jede Selektion ein Erkenntnisgewinn, denn wenn die Interessengruppen „blau“ und „grau“ lauten, dann ist die Einordnung einer Person in die Interessengruppe „blau“ – statt „grau“ – per se ein Erkenntnisgewinn, weil man daraus lernen kann, dass sie (zumindest aus der Sicht des Verantwortlichen) eher an blau als an grau interessiert ist.

- Und am Ende grüßt wieder das Wettbewerbsrecht

Das Wichtigste zum Schluss: Die Lösung der aufgeführten datenschutzrechtlichen Problemstellungen – in welcher Richtung auch immer – wird gleichwohl in vielen Fällen einen Pyrrhus-Sieg darstellen. Denn im Gegensatz zum Datenschutzrecht, bei dem (vermeintlich, s. o. Fall 17) die Einwilligung und die Interessenabwägung – also „opt-in“ und „opt-out“ – gleichberechtigt nebeneinander stehen, fordert das Wettbewerbsrecht immer eine Einwilligung in die vom Gesetzgeber grundsätzlich (auch in B2B-Situationen) als „belästigend“ eingestufte Werbung. Diese Einwilligung muss ausdrücklich erfolgen, eine stillschweigende oder mutmaßliche Einwilligung reicht – mit einer Ausnahme – gerade nicht aus: Nach dem Inkrafttreten der DSGVO wird von vielen Juristen angenommen, dass im Bereich der elektronischen Medien die Voraussetzungen der DSGVO für eine wirksame Einwilligung auch und gerade für die wettbewerbsrechtliche Einwilligung gelten (da das Wettbewerbsrecht insoweit auf der alten E-Privacy-Richtlinie der EU basiert). Nur in einem Fall darf eine wettbewerbsrechtliche Einwilligung auch eine mutmaßliche Einwilligung sein, nämlich im (bereits oben angesprochenen) Bereich der Telefonwerbung gegenüber Unternehmen.

Selbst wenn also datenschutzrechtlich argumentiert werden kann, dass die Daten vom Betroffenen selbst, sei es auch im Einzelfall (Visitenkartenübergabe, zufälliges persönliches Kennenlernen) mit unausgesprochenem Zweckumfang, überlassen wurden und daher einer „positiven“ Interessenabwägung zugänglich sind, bedeutet dies noch lange nicht, dass wettbewerbsrechtlich eine (ausdrückliche) Einwilligung für jegliche E-Mail-Ansprachen zu Werbezwecken erteilt wurde. Der Hinweis der Maier GmbH in ihrer Außenkommunikation auf die Nutzung der personenbezogenen Daten zu Werbezwecken kann daher als solcher keine Einwilligung im wettbewerbsrechtlichen Sinne ersetzen. Dies soll hier nicht im Einzelnen vertieft werden, zeigt aber, dass auch die Einhaltung des Datenschutzrechts oftmals nur die „halbe Miete“ ist und weitere Erwägungen anzustellen sind, die das Ergebnis der schön „zurechtgedrechselten“ DSGVO-Argumentationen hinterrücks aushebeln. Glücklicherweise sind Abmahnungen im Bereich der B2B-Werbung in der Praxis eher selten (mit Ausnahme

der Werbung für „Telefon- und Webverzeichnisdienste“, wenn man die Rechtsprechung ansieht) und die Sanktionen bei Verstößen gegen das Wettbewerbsrecht sind mit denen bei DSGVO-Verstößen wirtschaftlich kaum vergleichbar.

Fall 30:
Information nur gegen Daten

Praktischer Fall: Die Finanzberatung Maier GmbH stellt Interessenten auf ihrer Website wöchentlich den „Anlagetipp der Woche" zur Verfügung. Dieser wird in Form einer E-Mail verschickt und der Interessent muss sich zuvor im Double-Opt-In-Verfahren auf der Website anmelden. Dabei muss er eine Einwilligung erteilen, dass er auch mit der Zusendung von Newslettern und von Veranstaltungseinladungen der Maier GmbH einverstanden ist.

Hinter diesem Fall steht ökonomisch das weitreichende Thema „kostenlose" Leistung eines Anbieters (Verantwortlichen) gegen die Zurverfügungstellung personenbezogener Daten eines Betroffenen. Ein Tauschgeschäft mit dem „Grundwasser des 21. Jahrhunderts" (ein Begriff übrigens, den der Bundesdatenschutzbeauftragte dem Begriff „Öl des 21. Jahrhunderts" vorzieht): Der Verantwortliche gibt „irgendeine Leistung", der Betroffene gibt im Gegenzug „seine Daten", zu welchen (erklärten oder unerklärten faktischen) Zwecken auch immer. Datenschutzrechtlich geht es hier um das Schlagwort „Koppelungsverbot" im Sinne einer Koppelung der Erbringung einer Leistung gegenüber dem Betroffenen mit der Einwilligung des Betroffenen in eine Verarbeitung seiner Daten, die über das zur Leistungserbringung unmittelbar Erforderliche hinausgeht. Man könnte es (fast) auch „Erpressungsverbot" nennen, denn in der Sache soll dem Betroffenen eine weitergehende Einwilligung „abgepresst" werden. Das oben in Fall 17 besprochene „versteckte" Koppelungsverbot betrifft hingegen den Fall, dass eine über den Vertrag hinausgehende Einwilligungserklärung durch eine Interessenabwägung (mutmaßliche Einwilligung) ersetzt wird.

➢ Das „Koppelungsverbot"

Nun ist das Koppelungsverbot eigentlich gar kein Verbot. Die Regelung in Art. 7 Abs. 4 DSGVO besagt „nur", dass eine „erpresste" Einwilligung des Betroffenen nicht freiwillig ist und damit die Einwilligung als datenschutzrechtlicher Legitimationsgrund ausscheidet. Wer also als Verantwortlicher dem Betroffenen eine Einwilligung in eine Verarbeitung personenbezogener Daten „abpresst", die zur Erfüllung des Vertragszwecks nicht erforderlich sind, verfügt zwar über eine Einwilligung, aber über keine freiwillige – und damit über keine wirksame – Einwilligung.

In einem einfachen Beispiel könnte also ein Online-Shop, bei dem der Betroffene Besteck einkaufen möchte, die Annahme und Ausführung der Bestellung davon abhängig machen,

dass der Betroffene in die Verarbeitung seiner Kontaktdaten zu Zwecken des Direktmarketings durch diesen Online-Shop einwilligt. Zur Erfüllung des Vertrages ist das Direktmarketing schließlich nicht erforderlich. Aber Moment mal, das war doch im Rahmen der Interessenabwägung (s. oben Fall 29) und mit Einschränkungen auch im Wettbewerbsrecht erlaubt? Naja, eigentlich geht es ja um die „böseren" Fälle, in denen der Betroffene z. B. einwilligen soll, dass seine Kontaktdaten vom Betreiber des Online-Besteck-Shops an den Betreiber einer Glücksspielseite weitergegeben werden, der den Betroffenen dann mit Werbung „zuspammen" darf. Mit anderen Worten: Dort, wo eine Interessenabwägung zugunsten des Verantwortlichen ausgehen würde – etwa in den einschlägigen Direktmarketing-Fällen –, wird man wohl eine auf dasselbe Ziel gerichtete Einwilligungserklärung, selbst wenn diese über das zur Erfüllung des Vertrages Erforderliche hinausgeht, eigentlich nicht als „unfreiwillig" bezeichnen können. Sonst würde das die Einholung einer Einwilligung (noch) unattraktiver machen und außerdem das Gesamtgefüge aus der Balance bringen.

Der österreichische Oberste Gerichtshof hat dies allerdings in einer Entscheidung vom August 2018 strikter formuliert, nämlich sinngemäß wie folgt:

„Im Falle einer Koppelung der Einwilligung zu einer Verarbeitung vertragsunabhängiger personenbezogener Daten mit einem Vertragsschluss sind an die Beurteilung der „Freiwilligkeit" der Einwilligung strenge Anforderungen zu stellen. Es ist dabei grundsätzlich davon auszugehen, dass die Erteilung der Einwilligung nicht freiwillig erfolgt, wenn nicht im Einzelfall besondere Umstände für eine Freiwilligkeit der datenschutzrechtlichen Einwilligung sprechen."

➢ Datenlieferung als weiterer Vertragsinhalt

Nun kann die vom „Koppelungsverbot" eigentlich beabsichtigte Unwirksamkeit einer „abgepressten" Einwilligungserklärung, die über das zur Erfüllung eines Vertrages Erforderliche hinausgeht, im Wesentlichen auf zwei Arten „umgangen" werden.

In der ersten Variante kann der Vertrag – man müsste sagen „missbräuchlich" – von vornherein so strukturiert werden, dass er formal für seine Erfüllung die Verarbeitung der Daten erforderlich macht. Die Weitergabe der Kontaktdaten an den Betreiber der Glücksspielseite kann also schlicht zum Vertragsinhalt gemacht werden: „Gegenstand dieses Vertrages ist der Kauf von Besteck und die Weitergabe Ihrer Daten an interessierte Händler und Dienstleister". Das wäre dann gar kein Problem des „Koppelungsverbotes" mehr, denn der Verantwortlich benötigt ja gar keine Einwilligung für die Verarbeitung personenbezogener Daten, soweit diese für die Erfüllung eines Vertrags erforderlich ist (Art. 6 Abs. 1 S. 1 lit. a) DSGVO).

Der Verantwortliche muss die Daten dann sogar gerade an die bezeichneten Dritten weiterleiten, um seiner „vertraglichen Weiterleitungspflicht“ gegenüber dem Betroffenen nachkommen zu können. Mit der Freiwilligkeit einer Einwilligung hat das nichts zu tun. Die Erwägungsgründe der DSGVO führen zwar grundsätzlich zur „unangebrachten“ Verknüpfung zweier Sachverhalte aus, dass – neben dem „Koppelungsverbot“ – auch dann keine Freiwilligkeit vorliegt,

„wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist“.

Man würde also im Fall von Besteck und Glücksspiel – wohl unter Anwendung des „objektive Maßstabs der Vernunft“ (s. oben Fall 29) – eine „Entbündelung“ der Einwilligungserklärungen eigentlich für „angebracht“ halten müssen. Auch der österreichische Oberste Gerichtshof hat sich in der oben genannten Entscheidung ausdrücklich auf das Entbündelungsgebot berufen. Allerdings geht es beim Vertrag um Besteck und Glücksspiel gar nicht um eine Einwilligung in verschiedene Verarbeitungsvorgänge, sondern um eine „Vertragskombination“, die der Verantwortliche eigentlich im Rahmen der Vertragsfreiheit so definieren kann, wie er das möchte. Also eine „perfekte Umgehung“?

➢ Vertragskontrolle nach Datenschutzrecht

Nicht wirklich. Denn auch die Vertragsfreiheit ist zwischenzeitlich unter den Beschuss des Datenschutzrechts geraten, und zwar im Zusammenhang mit der Frage, was wirklich für den Vertrag „erforderlich“ ist. Nicht nur viele Kommentatoren versuchen, Ansätze in Richtung einer Einschränkung der vertraglichen Definitionsfreiheit zu entwickeln, etwa indem sie auf den „Kern des Vertrages“ abstellen, die Lösung im AGB- bzw. EU-Verbraucherschutzrecht suchen oder auf die Grundprinzipien der DSGVO wie „Treu und Glauben“, Zweckbindung und Datenminimierung abstellen. Auch der Europäische Datenschutzausschuss versucht in diesem Zusammenhang in seinen Empfehlungen vom April 2019, eine eigene „datenschutzrechtliche Inhaltskontrolle“ zu etablieren, indem es ausführt (man achte auf das Schlüsselwort „künstlich“/„*artificially*“):

„Contracts for digital services may incorporate express terms that impose additional conditions about advertising, payments or cookies, amongst other things. A contract cannot artificially expand the categories of personal data or types of processing operation that the controller needs to carry out for the performance of the contract within the meaning of Article 6(1)(b).

The controller should be able to justify the necessity of its processing by reference to the fundamental and mutually understood contractual purpose. This depends not just on the controller's perspective, but also a reasonable data subject's perspective when entering into the contract, and whether the contract can still be considered to be 'performed' without the processing in question. Although the controller may consider that the processing is necessary for the contractual purpose, it is important that they examine carefully the perspective of an average data subject in order to ensure that there is a genuine mutual understanding on the contractual purpose."

Lediglich auf den letztgenannten Aspekt – die Sichtweise des Betroffenen (auch wenn es „künstlich" ist?) – beschränkt sich das bayerische Landesamt für Datenschutzaufsicht in seinem Tätigkeitsbericht 2017/2018:

„Wir gehen bei solchen Geschäftsmodellen von einer vertraglichen Grundlage für die Verarbeitung der personenbezogenen Daten gemäß Art. 6 Abs. 1 Satz 1 Buchstabe b DS-GVO aus, wenn die ausbedungene Gegenleistung des Nutzers, d. h. die Zustimmung zur Verarbeitung seiner Daten für die Zusendung eines Werbe-Newsletters, bei Vertragsabschluss über die vereinbarte kostenlose Dienstleistung klar und verständlich dargestellt wird und damit ein Nutzer eine sachgerechte Entscheidungsgrundlage hat."

In einer Entscheidung vom Juni 2019 hat das OLG Frankfurt demgegenüber keine Bedenken gegen die Freiwilligkeit einer Einwilligung erhoben, wenn die Teilnahme an einem Gewinnspiel von der Einwilligung in den Erhalt künftiger E-Mail-Werbung abhängig gemacht wird. Diese Entscheidung wurde häufig mit dem „Koppelungsverbot" in Verbindung gebracht, beschäftigt sich aber nicht mit den Voraussetzungen und Folgen von Art. 7 Abs. 4 DSGVO, sondern allgemein mit dem Merkmal der Freiwilligkeit (Art. 4 Nr. 11 DSGVO). Nach dem OLG Frankfurt muss und kann der Verbraucher selbst entscheiden, ob ihm die Teilnahme am Gewinnspiel die Preisgabe seiner Daten „wert" ist. Das wettbewerbsrechtlich geprägte Urteil geht auf die Frage, ob hier vielleicht ein gegenseitiger Vertrag vorlag, nicht ein.

Hinsichtlich Art. 7 Abs. 4 DSGVO aber wäre es sicherlich besser gewesen, wenn sich der Gesetzgeber über den zugrundeliegenden Mechanismus und die verschiedenen Fallgestaltungen genauer Gedanken gemacht hätte, anstatt dass nun gerätselt wird, anhand welcher Gesichtspunkte hier die Trennlinie verläuft. Man mag sich die entsprechenden Beispiele 6 bis 8 der Empfehlungen des Europäischen Datenschutzausschusses vom April 2019 vor Augen führen und fragen, ob man die Wertungsentscheidungen der dortigen „Musterlösungen"

jeweils für unmittelbar einleuchtend hält. Außerdem, aber das nur am Rande, ist völlig unverständlich, weshalb der Gesetzgeber den obigen Grundsatz des „Entbündelungsgebots" nur in die Erwägungsgründe, das (fälschlicherweise) sogenannte „Koppelungsverbot" aber daneben auch in den Verordnungstext selbst geschrieben hat. Das Problem des „künstlichen Aufblasens des Vertragsgegenstandes" wird jedenfalls von der DSGVO nicht gelöst und wäre vermutlich mit datenschutzrechtlichen Mitteln auch kaum zu lösen.

- Daten als Gegenleistung

Oben war davon die Rede, dass die Unwirksamkeit einer „abgepressten" Einwilligungserklärung auf zwei Arten „umgangen" werden kann. Die erste Variante war die Definition des Vertrages dergestalt, dass dieser die Verarbeitung der (weiteren) Daten über den „ursprünglichen" Vertragszweck hinaus notwendig macht, weil ein zweiter Vertragszweck bzw. Vertragsgegenstand hinzugefügt wird. Vertragsrechtlich würde man die Daten als „Beistellleistung" des Betroffenen bezeichnen. Die zweite Variante – so auch im Ausgangsfall – geht demgegenüber dahin, dass der Verantwortliche eine Leistung anbietet, für die er erklärtermaßen als Gegenleistung „nur" die Daten (und kein Entgelt) erwartet. Vertragsrechtlich sind dann die Daten als solche die Gegenleistung, d. h. es handelt sich um einen Tausch Leistung gegen Daten. Der Betroffene bezahlt also derartige – ggf. werbefinanzierte – Inhalte und Dienstleistungen „mit seinem guten Namen", sprich mit seinen Daten.

Man kann nun argumentieren, dass ein solches Tauschgeschäft – die Nutzung einer „kostenlosen" App wird gegen die Möglichkeit der weiteren Verwendung der dort einzugebenden Daten gestattet – ein (gegenseitiger) Vertrag ist, dann geht es (wiederum) begrifflich nicht um eine Einwilligung und damit würde auch das Koppelungsverbot keine Rolle spielen. Vertragsrechtlich würde man sagen: Wenn jemand sich weigert, seine personenbezogenen Daten zum Zweck des (Tausch-)Vertrages herzugeben – dies ist Vertragserfüllung, keine Einwilligung als Legitimationsgrundlage im datenschutzrechtlichen Sinne –, muss der Verantwortliche auch die Bereitstellung der Information, der Dienstleistung oder einer App nicht erbringen. Das Problem dabei ist nur, dass die gegenseitige Erbringung der vertraglichen Leistungen in der Praxis häufig formal als „Einwilligung" bezeichnet und ausgestaltet wird. So wurde dies auch im Ausgangsfall gehandhabt (förmliche „double opt-in"-Zustimmungserteilung, die allerdings das Datenschutzrecht für Einwilligungen formal – wenn man einmal von der Beweisbarkeit absieht – gar nicht verlangt, sondern nur das Wettbewerbsrecht). Diese übliche äußere Gestalt lässt das Tauschgeschäft – im Ausgangsfall die vertragsgemäße Zurverfügungstellung der Kontaktdaten des Betroffenen für Newsletter-Zusendungen etc. gegen die Übermittlung der gewünschten Anlagetipps der Maier GmbH – datenschutzrechtlich eher als Gratisleistung, die von der Erteilung einer Einwilligung abhängig gemacht wird, erscheinen.

Das verwundert nicht, denn die „Konstruktion“ des konkreten Tauschgeschäfts, bei dem die Einwilligung durch die Verarbeitung zu den – frei definierten – Zwecken des Tauschgeschäfts (Vertragserfüllung) ersetzt wird, mag dem einen oder anderen (Nicht-)Juristen „kontraintuitiv“ erscheinen. Selbst das Kammergericht in Berlin hat in seiner Google-AGB-Entscheidung aus dem März 2019 in einer Seitenbemerkung ausgeführt, dass die von einem Betroffenen erhobenen Daten nicht als „Entgelt“ für anderweitige Leistungen angesehen werden können, da ja der Betroffene seine „Einwilligung“ jederzeit widerrufen könne. Eine „Leistung“, die der Betroffene jederzeit zurückziehen kann, sei aber kein taugliches Entgelt. Von einem Entgelt könne nur die Rede sein, wenn sich der Nutzer zur Einwilligung in die Nutzung seiner Daten verpflichten würde. Hier werden also die Legitimationsgrundlagen Einwilligung und Vertrag – letzterer lässt gerade keinen isolierten datenschutzrechtlichen „Widerruf“ zu, sondern nur die Instrumente des Vertragsrechts wie Kündigung – vermischt.

Hingegen tendieren die Datenschutzbehörden selbst bei einer eher datenschutzfokussierten „Lesart“ einer Verknüpfung der Informationsübermittlung an eine Einwilligung im datenschutzrechtlichen Sinne – also ohne Rückgriff auf einen gegenseitigen Tauschvertrag – dazu, diese im Ergebnis in gewissem Rahmen zuzulassen. Wie dieser Rahmen allerdings im Einzelnen aussieht, ist unklar. Gerade im Beispielsfall oben wird argumentiert, dass es – letztlich um die „Ernsthaftigkeit“ des Angebots „Information gegen Daten“ zu unterstreichen – notwendig sei, dem Benutzer eine kostenpflichtige Alternative ohne die Notwendigkeit der Erhebung weiterer Daten anzubieten. Es müsse also auch immer eine „datensparsame“ Alternative geben, d. h. im Grunde wird eine Vertragstypalternative eingefordert („Informationskauf“ statt Tausch). Woraus genau die Notwendigkeit einer solchen „Zwangs-Handlungsalternative“ hergeleitet wird, ist nicht ganz klar.

Nach einem Bescheid der österreichischen Datenschutzbehörde vom November 2018 wird dies unter dem Gesichtspunkt der Freiwilligkeit behandelt, d. h. die Alternative, seine Daten „herzugeben“ oder (gar) nicht, ist keine echte Alternative, sondern nur, seine Daten „auf diese oder andere Weise herzugeben“. Dies steht aber nicht nur nicht in der DSGVO, sondern auch im Widerspruch zu der an anderer Stelle von den Datenschutzbehörden vertretenen Auffassung, es dürfe gar keine Einwilligung eingeholt werden, soweit ein Vertrag die Datenverarbeitung legitimiere. Die Einholung der Einwilligung sei dann gar nicht „erforderlich“ (eine Voraussetzung, die sich aber wiederum gerade nicht aus dem Text der DSGVO ergibt). Wichtig ist trotz aller Unklarheiten aber zumindest entsprechende Transparenz gegenüber dem Betroffenen. Auf diesen Aspekt kommen wir unten noch zurück.

➢ Der „Weichmacher“ in Art. 7 Abs. 4 DSGVO

Selbst wenn man in derartigen Fallgestaltungen davon ausgehen würde, dass es datenschutzrechtlich einer Einwilligung bedarf und damit das „Koppelungsverbot“ zu prüfen ist, muss dennoch nach dem Text der DSGVO die zur Unfreiwilligkeit der Einwilligungserklärung führende Verknüpfung zwischen Vertragserfüllung und Einwilligung nur „in größtmöglichem Umfang“ berücksichtigt werden. Mit anderen Worten: Nicht jede Koppelung ist strikt verboten, denn es heißt gerade nicht kategorisch: „Wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind, ist die Einwilligung nicht freiwillig erteilt worden“. Was diese Formulierung der Berücksichtigung der Verknüpfung „in größtmöglichem Umfang“ im Einzelnen bedeutet, ist unklar. Der Begriff wird in der Kommentarliteratur durch die mindestens ebenso diffuse Formel ersetzt, dass der Verantwortliche nur *„angemessene Anstrengungen unternehmen soll“*, um dem Betroffenen auch bei Abschluss eines Vertrages die Wahlfreiheit zu erhalten, ob er über den Vertrag hinausgehende Einwilligungen erteilt oder nicht. Aber kann es datenschutzrechtliche Einwilligungen über den Vertrag hinaus geben, die der Verantwortliche so „bitterlich benötigt“, dass es den Nachteil der Koppelung gegenüber dem Betroffenen, der dann Vertrag und Einwilligung nur „im Paket“ akzeptieren muss, rechtfertigt? Anders ausgedrückt: Wenn ein Vertrag eine bestimmte Verarbeitung bestimmter personenbezogener Daten nicht erfordert, welche Verarbeitung welcher personenbezogener Daten könnte dann dennoch so wichtig sein, dass der Vertragspartner diese Daten doch „haben muss“?

➢ Transparenz gegenüber dem Betroffenen

Daneben ist noch – wie oben angedeutet – auf einen anderen, in der Praxis sehr bedeutsamen Aspekt im Zusammenhang mit der Einwilligung hinzuweisen: Diese ist auch dann unwirksam, wenn der Betroffene nicht ausreichend konkret und transparent informiert wurde. Auch hier gilt es, missbräuchliche von „verständlichen“ Fallgestaltungen abzuschichten. Missbräuchlich sind Fälle „gewollter Intransparenz“, in denen also die maßgebliche Information schon mitgeteilt wird, aber so verschlungen und versteckt, dass der Betroffene unter normalen Umständen nicht „durchblicken“ wird. Die französische Datenschutzaufsichtsbehörde CNIL hat im Januar 2019 Google mit einer Strafe in Höhe von EUR 50 Mio. belegt, weil der Zweck der Datenerhebung zu allgemein und vage beschrieben worden sei und außerdem

„wesentliche Informationen, wie die Zwecke der Datenverarbeitung, die Aufbewahrungsfristen oder die Kategorien von personenbezogenen Daten, die für die Personalisierung der

Anzeigen verwendet werden, zu sehr auf mehrere Dokumente verteilt sind, mit Buttons und Links, auf die geklickt werden muss, um auf zusätzliche Informationen zuzugreifen".

Auch seien die Optionen zur Steuerung der Aktivität von Google – also zur Reichweite der Einwilligung – zu versteckt und es bleibe unklar, welche anderen Dienste und Webseiten (wie Youtube, Maps, Drive etc.) in die Verarbeitung der personenbezogenen Daten involviert sind. Die Konsequenz dieser Erkenntnis ist, dass keine wirksame Einwilligung der Nutzer vorliegt und die personenbezogenen Daten entsprechend nicht verarbeitet werden dürfen.

Welche Informationen dem Betroffenen vorliegen müssen, damit eine informierte Einwilligung vorliegen kann, wurde oben in Fall 8 erörtert. In Bezug auf die – neben diesen „Einwilligungsinformationen" – zu erteilenden Pflichtinformationen soll aber gleichwohl der oben zu Fall 29 beschriebene „Medienbruch" bei der Aufklärung des Betroffenen prinzipiell zulässig sein, d. h. eine Aufteilung der relevanten Information auf verschiedene Informationsorte wäre nicht schlechthin unzulässig. Wo genau die Grenzen der Transparenz liegen bzw. wie detailliert die beabsichtigte Verarbeitung beschrieben werden muss, bleibt demnach offen.

➢ Informationsmängel beim Verantwortlichen

Neben solchen, möglicherweise „gewollten" Intransparenzen gibt es allerdings auch Informationsmängel, die selbst der Verantwortliche nicht abstellen kann. Wenn der Verantwortliche klar darlegt, dass er ergebnisoffene „big data"-Analysen mit den personenbezogenen Daten vorhat, also im Klartext noch nicht genau weiß, für welche Erkenntnisse er die Daten verwenden wird, ist dann eine Einwilligung hierzu undenkbar? Wenn man in diesem Fall fordert, dass die Voraussetzungen, Konsequenzen und Algorithmen von Datenanalysen bzw. einer Profilbildung genau im Vorhinein beschrieben werden müssen, wird eine „Blanko-Einwilligung" des Betroffenen rechtlich nicht erreichbar sein. Wenn die Alternative nur darin bestehen kann, dass der Betroffene in die einzelnen „Verarbeitungsstufen" gesondert einwilligen muss, sobald diese – anhand des Ergebnisses der vorherigen Stufe – konkret genug beschrieben werden können, wird das beim Verantwortlichen kaum zu implementieren sein.

Ebenso kann der Verantwortliche schwerlich die Einwilligung zu Datenverarbeitungsvorgängen einholen, die er selbst nicht einmal kennt (s. dazu auch oben die Fälle 13 und 16). Im Datenschutz- und Informationsfreiheitsbericht 2019 der Landesdatenschutzbeauftragten von

Nordrhein-Westfalen wird etwa der Fall „Rezeptbestellungen mittels Whatsapp“ wiedergegeben, bei dem ein Patient der Apotheke ein Rezept über Whatsapp zukommen lässt. Die Tatsache, dass Whatsapp zumindest nach eigenen Angaben eine Ende-zu-Ende-Verschlüsselung etabliert hat, wird hier nicht weiter aufgegriffen. Stattdessen führt die Landesdatenschutzbeauftragte aus:

„Die Einholung einer gemäß Art. 9 Abs. 2 Buchstabe a) DS-GVO erforderlichen informierten Einwilligungserklärung dürfte in der Praxis eher schwierig sein, weil die Apotheken selbst tatsächlich keine ausreichenden Aussagen über die Datenverarbeitung bei dem genutzten Messengerdienst treffen können.“

Vielleicht liegt hier auch ein Fall der „gemeinsamen Verantwortlichkeit“ vor? Wie auch immer: Wer nicht weiß, wie etwas funktioniert, das personenbezogene Daten verarbeitet, kann auch keine wirksame Einwilligung des Betroffenen für die Nutzung dieses „etwas“ erlangen. Dabei bleibt gleichwohl offen, was genau der Verantwortliche nun wissen müsste, um den Betroffenen aufzuklären, denn anscheinend wird hier ein weitergehender Maßstab vorausgesetzt als die DSGVO ausdrücklich vorsieht (Speicherdauer? – s. o.). Und eine konkludente Einwilligung durch bloße Nutzung könne, so die Landesdatenschutzbeauftragte weiter, auch nicht unterstellt werden, weil „die Annahme einer bloß konkludenten Willensbekundung dem Datenschutzrecht fremd ist“. Wenn dem so wäre, dürfte wohl Whatsapp auch zwischen privaten Personen (s. oben Fall 18) weitgehend nicht mehr angewandt werden können.

- Widerruf der Einwilligung

Anlässlich einer Entscheidung der polnischen Datenschutzaufsichtsbehörde vom November 2019 soll hier noch ergänzend kurz auf die Umstände des Widerrufs einer erteilten Einwilligung (Art. 7 Abs. 3 DSGVO) eingegangen werden. Der Verantwortliche hatte den Betroffenen einen Link zur Verfügung gestellt, mit dessen Auswahl die Betroffenen ihre Einwilligung widerrufen konnten. Allerdings führt das Anklicken des Links nicht zum Widerruf, sondern zu „irreführenden“ Informationen sowie zu einer „Zwangsangabe“ über den Grund des Widerrufs. Wer keinen Grund angab, konnte nicht widerrufen. Diese Gestaltung seitens des Verantwortlichen wurde – natürlich – als vorsätzlicher Verstoß gegen Art. 7 Abs. 3 DSGVO gewertet: Der Widerruf muss für den Betroffenen so einfach wie die Erteilung der Einwilligung sein.

Fall 31:
Untersuchung mit oder ohne Lupe?

Praktischer Fall: Die Huber AG hat von Herrn Rolf Maier und seinem Sohn sämtliche Geschäftsanteile an der Maier GmbH erworben. Der Kaufpreis beruhte auf einer Unternehmensplanung der beiden Verkäufer, die einen bestimmten Umsatz und ein bestimmtes Ergebnis der Maier GmbH prognostiziert. Nach dem Erwerb bleibt Herr Rolf Maier zunächst weiter Geschäftsführer der Maier GmbH, während sich die Umsätze und das Ergebnis nicht im Ansatz planungsgemäß entwickeln, obwohl keine einschneidenden wirtschaftlichen Entwicklungen vorliegen. Der Sohn von Herrn Rolf Maier, vormals im Rechnungswesen des Unternehmens beschäftigt, ist nach dem Verkauf als Privatier tätig. Der Vorstand der Huber AG vermutet, von den Verkäufern „betrogen worden zu sein", da diese eine völlig unrealistische Planung aufgestellt haben. Daher ordnet der Vorstand eine Untersuchung des E-Mail-Verkehrs der Verkäufer sowie weiterer Mitarbeiter der Maier GmbH an, um Indizien für eine gezielte Täuschung der Huber AG zu suchen. Zu diesem Zweck werden die E-Mails der vergangenen Jahre von verschiedenen Personen, soweit noch in den dienstlichen E-Mail-Accounts vorhanden, „abgezogen" und durch eine beauftragte Wirtschaftsprüfungsgesellschaft mithilfe von Stichwortsuchen durchgesehen.

Die sich bei einer Durchsuchung von E-Mail-Accounts im Rahmen forensischer Untersuchungen stellenden datenschutzrechtlichen Problemstellungen sind vielschichtig. Das Bundesdatenschutzgesetz enthält den vielsagenden Satz:

„Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind."

Nun ist schon unklar, ob diese spezielle Regelung aus dem Beschäftigtendatenschutz für Geschäftsführer – also für Herrn Rolf Maier – gilt. Aus der oben zitierten Regelung ergibt sich daneben, dass nur personenbezogene Daten von „Beschuldigten" eingesehen werden können. Geht es um „Zeugen", ist die Einsichtnahme nicht auf Basis der Regelung rechtfertigbar. Weiter ist im Ausgangsfall unklar, ob der Verdacht einer Straftat vorliegt – notwendig sind entsprechende „tatsächliche Anhaltspunkte". Über Prognosen zukünftiger Unterneh-

mensentwicklung kann im Grunde nicht getäuscht werden, nur über die Prognosegrundlagen. Der Huber AG geht es unabhängig davon aber auch in erster Linie darum, festzustellen, ob sich Ansprüche gegen Herr Rolf Maier und seinen Sohn im Zusammenhang mit dem Anteilskauf ergeben könnten. Es geht also – aus der Perspektive der Maier GmbH als Arbeitgeber – um Ansprüche „zwischen Dritten". Der „Verdacht", von dem in der oben zitierten Regelung gesprochen wird, muss sich aber gerade auf eine im Beschäftigungsverhältnis begangene Straftat richten, d. h. es reicht nicht aus, wenn die beiden Protagonisten lediglich den „Verkäufer-Hut" auf hatten. Ob man aus dem Sachverhalt herauslesen kann, dass Herr Rolf Maier durch die „Fehlplanung" auch noch „parallel" seine Geschäftsführerpflichten im Verhältnis zur Maier GmbH verletzt hat, ist mehr als fraglich.

Schon unter dem alten Bundesdatenschutzgesetz war man der Meinung, dass die oben wiedergegebene Regelung – die es vor dem Inkrafttreten der DSGVO bereits gab – andere Legitimationsgrundlagen nicht hemmt. Man fragt sich aber schon, wozu die Regelung dann überhaupt nutzen soll, denn im Grunde konkretisiert sie ja nur die „Eckdaten" einer typischen Interessenabwägung. Ohne diese spezielle Regelung würde also das Ergebnis einer Interessenabwägung wohl kaum anders ausfallen. Bedeutet aber nun der Umstand, dass die Regelung nicht abschließend sein soll, dass man beliebige andere Interessenabwägungen anstellen darf? In denen es nicht um Straftaten und nicht um Beschuldigte geht?

In einem Urteil vom Januar 2019 hat das Bundesarbeitsgericht außerhalb der Spezialregelung zur Aufdeckung von Straftaten auf den allgemeinen Grundsatz der Erforderlichkeit für die Durchführung und Beendigung des Beschäftigungsverhältnisses verwiesen. Diese allgemeine Regelung in § 26 BDSG ist ihrerseits nur eine Ausprägung des Grundverständnisses der DSGVO, dass eine Verarbeitung rechtmäßig ist, die zur Erfüllung eines Vertrages erforderlich ist. Hierzu führt das Bundesarbeitsgericht aus:

„Zur Durchführung gehört die Kontrolle, ob der Arbeitnehmer seinen Pflichten nachkommt, zur Beendigung im Sinne der Kündigungsvorbereitung die Aufdeckung einer Pflichtverletzung, die die Kündigung des Arbeitsverhältnisses rechtfertigen kann. [...] Der Begriff der Beendigung umfasst dabei die Abwicklung eines Beschäftigungsverhältnisses. Der Arbeitgeber darf deshalb alle Daten speichern und verwenden, die er benötigt, um die ihm obliegende Darlegungs- und Beweislast in einem potenziellen Kündigungsschutzprozess zu erfüllen."

Auch außerhalb eines Verdachts strafbarer Handlungen darf also die Information, die für den Ausspruch einer Kündigung und zur Beweisführung in einem späteren Prozess gegen den

Mitarbeiter erforderlich ist, im Rahmen einer unternehmensinternen Untersuchung erhoben und verwertet werden. In diesem Rahmen liest nun das Bundesarbeitsgericht den Begriff „erforderlich“ als „verhältnismäßig“ im Sinne der klassischen verfassungsmäßigen Verhältnismäßigkeitsprüfung:

„Die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten müssen geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen sein, um den erstrebten Zweck zu erreichen.“

Die hier im Rahmen der „Erforderlichkeit“ vorzunehmende Interessenabwägung ist datenschutzrechtlich zwar eher der Legitimationsgrundlage der Interessenabwägung als der Vertragserfüllung zuzuschlagen, aber das Bundesarbeitsgericht ist ja nicht gezwungen, dies genauer voneinander abzuschichten. Jedenfalls ist im Rahmen dieser Interessenabwägung nach dem Bundesarbeitsgericht aufseiten des Arbeitnehmers dessen „Privatheitserwartung“ in die Abwägung einzustellen. Dieses Interesse hindert den Arbeitgeber aber nur daran, „ins Blaue hinein“ oder beim Verdacht „bloß geringfügiger Verstöße“ eine heimliche Überwachung (und in diesem Rahmen Beweissicherung) durchzuführen. Daraus ergibt sich zweierlei: Erstens können offen kommunizierte Maßnahmen und Überwachungsmaßnahmen, die alle Arbeitnehmer gleichermaßen betreffen, auch ohne irgendeinen Anfangsverdacht erlaubt sein, wenn das „Privatheitsinteresse“ nicht verletzt wird (z. B. keine privaten Dateien auf einem Rechner durchsucht werden). Durch die offene Kommunikation gegenüber dem Arbeitnehmer kann dieser sich auf die Untersuchung „vorbereiten“ und private Daten in einen als privat gekennzeichneten Bereich verschieben. Und zweitens können bei einem durch Tatsachen begründeten Anfangsverdacht einer Pflichtverletzung im Rahmen des Beschäftigungsverhältnisses weitergehende Prüfungen durchgeführt werden, wenn diese noch verhältnismäßig sind.

In dem Sachverhalt, der der Entscheidung des Bundesarbeitsgerichts zugrunde lag, ging es um eine mögliche Pflichtverletzung des Arbeitnehmers, die möglicherweise zu einer Kündigung aus wichtigem Grund hätten führen können. Unklar bleibt, was nun für Personen gilt, die von vornherein nur als „Zeugen“ in Betracht kommen, d. h. denen von vornherein keine Pflichtverletzung vorgeworfen werden soll, die aber dennoch zielgerichtet – und nicht als Teil einer gegenüber allen Arbeitnehmern ausgeführten und vorher kommunizierten Überwachungsmaßnahme – untersucht werden sollen. Hier würde man wohl in der Praxis versuchen, sich eine Einwilligung einzuholen. Das führt jedoch zu drei Problemen. Erstens ist schon sehr zweifelhaft, ob eine solche Einwilligung freiwillig ist, also überhaupt rechtliche

Wirkung entfaltet. Zweitens wird die geplante Untersuchung durch die Frage nach der Bereitschaft der Betroffenen, eine Einwilligung zu erteilen, in gewissem Umfang „publik", d. h. die „Verdunkelungsgefahr" (insbesondere durch „Tipps" an die Betroffenen) steigt. Und drittens würde die Einwilligung sich ohnehin immer nur auf diejenigen Arbeitnehmer beziehen können, die einwilligen, und nicht auf die Dritten, mit denen sie per E-Mail kommuniziert haben. Dort ist also dann in jedem Fall eine Interessenabwägung vonnöten, und zwar von Interessen der Betroffenen, die man gar nicht kennen kann, weil man die E-Mail-Verkehre noch gar nicht untersucht hat. Hier beißt sich also die sprichwörtliche Katze in den Schwanz.

Daneben ist noch ein völlig anderer Aspekt zu berücksichtigen: Erlaubt der Arbeitgeber (die Maier GmbH) seinen Arbeitnehmern de facto – auch im Rahmen einer betrieblichen Übung entgegen entsprechender Verbotsklauseln im Arbeitsvertrag –, die dienstlichen E-Mail-Accounts auch für private Zwecke zu nutzen, kann vorrangig zum Datenschutzrecht das Telekommunikationsrecht Anwendung finden. Dies ist seit langem umstritten und der Gesetzgeber schaut zu. Das Bundesarbeitsgericht hatte diese Frage in dem oben genannten Fall nicht auf seinem „kritischen Pfad" durch den Sachverhalt, denn es ging um die Untersuchung der Dateien auf einem Laptop, nicht um ein E-Mail-Postfach. Wäre die Maier GmbH in diesem Fall tatsächlich mit der Telekom oder anderen Telekommunikationsunternehmen zu vergleichen, weil sie ihren Arbeitnehmern gegenüber als Telekommunikationsanbieter auftritt, könnten die E-Mails vom Fernmeldegeheimnis umfasst werden. Denn dieses besteht (nach der Rechtsprechung des Bundesverfassungsgerichts) so lange, bis der Adressat der E-Mail alleine über den Zugriff entscheiden kann. Ist es also möglich, „von außen in den Account hineinzusehen", etwa durch entsprechende Administratorenrechte, so könnte man argumentieren, dass das Fernmeldegeheimnis noch entsprechend weiter andauert. Ausnahmen vom Fernmeldegeheimnis bestehen aber nur in sehr engen Grenzen, etwa beim Verdacht des Erschleichens von Telekommunikationsdienstleistungen – ähnlich einer „Schwarzfahrt" mit öffentlichen Verkehrsmitteln. Interessenabwägungen oder die Nutzung von Erlaubnisregelungen wie die oben zitierte aus dem Bundesdatenschutzgesetz sind dann (eigentlich) nicht möglich. Es bleibt dann nur, die Einwilligung des Betroffenen – und möglicherweise auch die des Kommunikationspartners – einzuholen und damit die Untersuchungstätigkeit gegenüber dem „Beschuldigten" oder gegenüber „Zeugen" transparent zu machen.

Fall 32:
Hin und her ist nicht schwer

Praktischer Fall: Die Huber AG stellt Bett- und Unterwäsche her und vertreibt diese im Wesentlichen über einen Online-Shop. Sie lässt sämtliche Daten über die getätigten Verkäufe an ihre Kunden, unter denen sich auch viele Privatpersonen befinden, in eine intern bei der Huber AG „data lake" getaufte Datenbank fließen. Dabei werden Name und sonstige personenbezogene Daten des jeweiligen Kunden entfernt und die ursprünglichen Daten über die Verkäufe in den Produktivsystemen der Huber AG nach Ablauf der Gewährleistungsfrist gelöscht. Im „data lake" werden nur Daten wie PLZ des Kunden, bestellte Artikel, Datum und Uhrzeit der Bestellung, Zahlungsmittel, Reklamationshäufigkeit etc. gespeichert, ohne dass die Huber AG zurückverfolgen könnte, wer der Kunde ist. Die Huber AG lässt immer wieder von ihr so bezeichnete „big data"-Analysen erstellen, um das Verhalten ihrer Kunden besser vorhersagen zu können, und veräußert die Daten hin und wieder auch für einen kleinen Obolus an interessierte Dritte. Irgendwann erwirbt die Huber AG sämtliches Vermögen der Maier GmbH („Asset Deal"), die ähnliche Waren herstellt und in einer Datenbank über sämtliche Daten zu den von ihr jemals getätigten Verkäufern an ihre Kunden verfügt.

In den bisherigen Fällen war hin und wieder von pseudonymen Daten die Rede. Pseudonym bedeutet, dass die Zuordnung eines Datums (z. B. Schuhgröße 43) zur Identität einer konkreten Person (z. B. Herr Rolf Maier) über eine Zuordnungsinformation (z. B. „1234") erfolgt. Die Schuhgrößen verschiedener Personen können nun in einer Datei (man könnte diese als „Primär-Datenbank" bezeichnen) nur mit der jeweiligen Zuordnungsinformation verknüpft werden (also „1234 trägt Schuhgröße 43"). In einer anderen Datei (man könnte diese als „Zuordnungs-Datenbank" bezeichnen) werden dann die Zuordnungsinformationen mit der Identität einer natürlichen Person verknüpft (also „1234 ist Herr Rolf Maier"). Wenn diese Datenbanken ausreichend getrennt voneinander vorgehalten werden, sind die Daten der Primär-Datenbank „nur noch" pseudonym. Dabei gibt es zwei Arten von Pseudonymisierung: Die beiden Datenbanken können beim Verantwortlichen selbst getrennt sein – dann erschwert die Pseudonymisierung das Zusammenführen und schützt die Betroffenen etwas besser gegen die unberechtigte Verwendung ihrer Daten – oder die beiden Datenbanken liegen bei verschiedenen Verantwortlichen. Im letzteren Fall sollte man meinen, dass die Primär-Datenbank für deren Besitzer „anonym" (die Datenschutzbehörden sprechen hier aber auch von „verschleiernder Pseudonymisierung") sind: Er weiß nicht, wer „1234" ist, weil er nicht im Besitz der Zuordnungs-Datenbank ist.

➢ Anonyme Daten

Datenschutzrechtlich sind anonyme Daten solche, die keinen Personenbezug (mehr) aufweisen, und zwar weder aktuellen noch potentiellen Personenbezug. Solche Daten sind datenschutzrechtlich nicht (mehr) geschützt. Man kann (datenschutzrechtlich) mit ihnen machen, was man will. Dies ergibt sich zwar nicht aus dem Text der DSGVO, aber aus der Definition des Begriffs der „personenbezogenen Daten" sowie aus Erwägungsgrund 26.

Allerdings ist eine wirklich erfolgreiche Anonymisierung nicht einfach zu erreichen. Die Crux ist mit dem Wörtchen „potentiell" verbunden. Jede Rekonstruierbarkeit des Personenbezuges muss sicher ausgeschlossen sein. Schon die typische „Verstümmelung" von IP-Adressen, die manche Anbieter von Cookie-Systemen anbieten, ist meist nicht mehr ausreichend für eine erfolgreiche Anonymisierung, da dem Verantwortlichen weitere Daten vorliegen, die in Kombination eine Identifikation des Benutzers erlauben. Das müssen keine „browser fingerprints" sein, die eine sehr individuelle Wiedererkennung ermöglichen. So führt die „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien" der Datenschutzkonferenz vom März 2019 aus:

„Darüber hinaus ist zu berücksichtigen, dass sich Nutzer in den allermeisten Fällen früher oder später an irgendeiner Stelle im Web registrieren und in diesen Fällen auch eine Verknüpfung mit E-Mail-Adressen, Klarnamen oder Offline-Adressen möglich ist. Auf die Kenntnis des bürgerlichen Namens zur Identifikation von betroffenen Personen kommt es aber beim Personenbezug nicht an. Wenn die Nutzung des Webs, wie bei vielen Menschen, einen großen Teil der Lebenswirklichkeit widerspiegelt, dann ist es relevant, ob die Nutzer über ihre Online-Kennungen bestimmbar oder adressierbar sind."

➢ Attribute-Muster und Identifizierbarkeit

Diese Schlussfolgerung dürfte nicht ganz richtig sein, denn ein „personenbezogenes Datum" liegt nicht vor, wenn es sich bloß auf „irgendeine lebende Person" bezieht, sondern nur dann, wenn die Person – mit ihrem bürgerlichen Namen – identifizierbar ist. Sonst gäbe es schließlich gar keine anonymen Daten mehr, die vom Erwägungsgrund 26 wie folgt charakterisiert werden:

„Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden

sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten [...].“

Ist die Person allerdings identifizierbar, dann kommt es richtigerweise nicht mehr darauf an, ob der bürgerliche Name tatsächlich nun identifiziert wurde oder nicht.

Um dem etwas auf den Grund zu gehen, sollte man sich eine in „Nature Communications“ veröffentlichte Studie (*„Estimating the success of re-identifications in incomplete datasets using generative models“*) vor Augen halten, die einen statistischen Effekt im Zusammenhang mit der Identifizierbarkeit von Personen herausgearbeitet hat. Die Kernaussage der Studie bestand darin, dass in einer – vermeintlich – anonymisierten Datenbank mit den drei Attributen Postleitzahl, Geschlecht und Geburtsdatum eine 81 %-Wahrscheinlichkeit der Re-Identifikation besteht, die sich bei 15 demografischen Merkmalen auf 99,98 % erhöht. Dies führt zum Begriff der k-Anonymität, den Wikipedia wie folgt definiert:

„Eine Veröffentlichung von Daten bietet k-Anonymität, falls die identifizierenden Informationen jedes einzelnen Individuums von mindestens k-1 anderen Individuen ununterscheidbar sind und somit eine korrekte Verknüpfung mit den zugehörigen sensiblen Attributen erschwert wird. Der Buchstabe k stellt somit einen Parameter dar, der im konkreten Fall durch eine natürliche Zahl ersetzt wird. Ein größeres k repräsentiert in diesem Kontext eine größere Anonymität.“

Die Re-Identifizierung von Personen anhand ihrer Attribute ist zunächst nicht sehr verwunderlich. Wenn zu einer Person 15 Attribute gespeichert werden, ergeben die Attribute auch dann ein personenspezifisches „Muster“, wenn der Name der Person entfernt wird. Je mehr Attribute den „Fingerabdruck“ ausmachen, desto feingranularer und damit individueller wird der „Attribute-Fingerabdruck“. Dasselbe gilt für IP-Adressen oder sonstige „Identifier“, d. h. das Attribute-Muster stellt letztlich als solches ein Pseudonym dar. Es bleibt aber das Problem, dass jemand, der eine Person anhand ihres Attribute-Musters in einer Datenbank „wiedererkennt“, aber nicht weiß, wer derjenige ist, nur weiß, dass er es mit derselben Person zu tun hat, aber nicht, wie die Person heißt. Dasselbe gilt ja auch für (statische) IP-Adressen beim Tracking: Der Webseiten-Betreiber erkennt die IP-Adresse wieder („der hat hier schon einmal gesurft“), weiß aber nicht, wer das ist. Wenn nun ein Attribut die Adresse und ein weiteres Attribut die Nummer der Wohnung im Mehrfamilienhaus ist, lässt sich diese Unkenntnis natürlich leicht beseitigen: Man fährt hin und sieht nach, wer da auf dem Klingelschild steht. Bei IP-Adressen, demografischen oder medizinischen Attribute-Mustern kann

das aber für den einzelnen Verantwortlichen durchaus schwer bis unmöglich sein, die Identität (Name) herauszufinden, schon gar bei einer größeren Personenanzahl.

Für die Re-Identifizierung durch ein „Mapping" der Attribute-Muster sind also drei Informations-Sets notwendig: Ein „namenloses" Attribute-Muster in einer Zieldatenbank („Eine Person wohnt im PLZ-Bezirk 12345, ist männlich, ist am 01.01.1950 geboren und hat Schuhgröße 43") mit einer Zusatzinformation („Diese Person hat graue Haare"), ein entsprechendes Such-Muster („Ich kenne eine Person, die im PLZ-Bezirk 12345 wohnt, männlich ist, am 01.01.1950 geboren ist und Schuhgröße 43 hat") und die Verknüpfung mit einem Namen („Die Person, die ich kenne, ist Herr Ferdinand Müller"). Würde die Zieldatenbank keine weiteren Attribute aufweisen, so würde sich der Erfolg nur in der Kenntnis ausdrücken, nun zu wissen, dass ein Datensatz der Zieldatenbank Ferdinand Müller abbildet – für sich genommen keine besondere Erkenntnis, wenn sämtliche drei Informations-Sets schon vorlagen. Wüsste man zum Suchmuster nicht den Namen, so könnte man nur die Erkenntnis gewinnen, dass die Person, deren Identität (Namen) man nicht kennt (sondern nur ihr Attribute-Muster), graue Haare hat (vermutlich vom Datenschutz). Man würde also einer unbekannten Person weitere Attribute hinzufügen können und deren Identität weiterhin nicht kennen. Nur dann, wenn der Suchende sein Suchmuster mit einer Identität (Namen) verknüpfen kann, kann er aus der Zieldatenbank relevante auf die benannte Person bezogene Informationen herauslesen. Ansonsten ist (und bleibt) es eine „namenlose" Information. Ob diese im datenschutzrechtlichen Sinn „anonym" ist, ist aber eine andere Frage.

Die genannten Attribute bzw. deren Kombination zu Mustern können sehr vielfältig und unterschiedlich aussagekräftig sein. Dazu zählen Bewegungsprofile und (Kreditkarten-)Zahlungshistorien. Wenige solcher Daten genügen, um eine Person, deren Namen man kennt, in einer anderen Datenbank relativ zuverlässig re-identifizieren zu können, die über die gleichen Datenmuster (und zusätzliche Informationen) verfügt. „Relativ" deswegen, weil ein hundertprozentiges „Mapping" der Attribut-Muster, wie oben für einen „Bilderbuchfall" beschrieben, in der Praxis nicht immer (oder sogar eher selten) vorliegt. Wie (statistisch) „zuverlässig" das „Mapping" im Einzelfall genau sein muss, damit der eigentlich namenlose Datenbestand einer identifizierbaren Person zugeordnet werden kann und damit datenschutzrechtlich personenbezogen wird, ist unklar.

- Identifizierbare Person im Sinne der DSGVO

Die DSGVO nähert sich der Frage der Identifizierbarkeit nicht aus der Richtung der „Mapping-Genauigkeit" zwischen zwei Attribut-Mustern, sondern aus der Richtung, wann ein Bezug zwischen Daten und Person hergestellt werden kann, d. h. wann eine „identifizierbare

Person“ vorliegt. Im „Mapping“-Beispiel oben stünde also die Frage im Vordergrund, wie der Inhaber eines zunächst namenlosen Datensatzes an einen „mapping-fähigen“ Datensatz gelangen kann, der auch den Klarnamen enthält. Zur Veranschaulichung sei an die in der Einleitung zitierten Urteile des Europäischen Gerichtshofes und des Bundesgerichtshofes zum Thema dynamische IP-Adresse erinnert. Der Webseiten-Betreiber verfügte über ein namenloses Attribute-Muster in Form der (dynamischen) IP-Adresse (123.123.123.123) und eines Zeitstempels (01.01.2019, 12:00 Uhr) sowie über die – hier nicht so wichtige – Zusatzinformation, dass zu diesem Zeitpunkt von dieser IP-Adresse auf die Seite des Webseiten-Betreibers zugriffen wurde. Der Internet-Provider verfügt über dasselbe Attribute-Muster sowie die Verknüpfung mit dem Namen, sprich: „Ferdinand Müller war am 01.01.2019 um 12:00 Uhr die IP-Adresse 123.123.123.123 zugewiesen“. Hier lag die „Mapping-Genauigkeit“ bei 100 %. Auf die Frage, inwieweit hierbei dem Webseiten-Betreiber das Wissen des Internet-Providers „zugerechnet“ werden kann, kommen wir noch zurück. Wichtig ist, dass die „Mapping-Genauigkeit“ auch weniger sein kann. Im Beispiel könnte der Webseiten-Betreiber nur die ersten drei Bytes der IP-Adresse gespeichert haben, also 123.123.123.xxx – er kennt das letzte Byte nicht (mehr). Möglicherweise hat der Internet-Provider zum maßgeblichen Zeitpunkt 24 Adressen im Adressraum 123.123.123.0 bis 123.123.123.254 zugewiesen. Er kann also nur sagen, dass es „einer von 24 gewesen sein muss“. Welche „Mapping-Genauigkeit“ erreicht werden muss, sagt weder die DSGVO noch bislang ein Gericht.

Welche Anstrengungen können also dem Verantwortlichen unterstellt werden, um einen Bezug zwischen Datum und Person herzustellen, mit anderen Worten, um aus einer identifizierbaren Person eine identifizierte Person zu machen (auch wenn die Identifizierung dann tatsächlich gar nicht stattfindet)? Hierzu erläutert Erwägungsgrund 26:

„Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.“

Diese „Definition“, die nicht Teil des DSGVO-Texts selbst ist, strotzt vor unbestimmten Rechtsbegriffen. Auch ist die Bedeutung des Wortes „Aussondern“ als (einziger) Beispielsfall zunächst nicht klar. „Aussondern“ ist im Kontext des Lebenszyklus‘ von Akten wahlweise

die Archivierung oder Vernichtung der Akte. Mit der Identifizierung einer Person hat das aber wenig zu tun. Eher verständlich ist die englische Fassung („*singling out*"), die auch mit „auswählen" bzw. „herausgreifen" übersetzt werden kann. Gemeint ist demnach ein Auswählen oder Herausgreifen aus einer Masse von Daten anhand von definierten (Filter-)Kriterien bzw. Attributen, also sinngemäß mit dem oben beschriebenen „Mapping"-Prozess. Mit bestimmten Kosten und einem bestimmten Zeitaufwand könnte beispielsweise ein Unternehmen, das über viele Datensätze wie „Krankengeschichten" von Patienten verfügt, aber die Namen der Patienten nicht kennt und auch zu keinem Patienten in irgendeiner Beziehung steht, versuchen, weitere Datenbanken – auch kostenpflichtige – mit Klarnamen zu beziehen, um irgendein (statistisch mehr oder weniger gutes) „Mapping" zu betreiben und so den Namen des jeweiligen Patienten herauszufinden.

Dies wirft allerdings eine weitere Frage auf: Ist die Bewertung nur für einen Datensatz eines Betroffenen oder für die Gesamtheit der beim Verantwortlichen vorliegenden Datensätze zu bestimmen? Wenn der Aufwand für einen Datensatz verhältnismäßig groß ist, wird er für eine Masse von Datensätzen unverhältnismäßig sein und dann nicht mehr als taugliches Identifizierungsmittel in Betracht kommen. In den Entscheidungen des Europäischen Gerichtshofes und des Bundesgerichtshofes wurde diese Frage dahingehend beantwortet, dass der Aufwand für den einzelnen Datensatz zu bestimmen ist. Selbst wenn für sämtliche gleichartigen Datensätze der (Gesamt-) Aufwand, an die Identität sämtlicher Betroffenen zu gelangen, unverhältnismäßig groß bzw. das „Mapping" sogar praktisch unmöglich wäre, ist dies also demnach irrelevant. Entscheidend ist, dass es isoliert für den einzelnen Datensatz einen irgendwie noch plausiblen Weg zur Identifizierung – im Sinne einer „Namensgebung" – gibt, selbst wenn (im Beispiel der genannten Gerichtsentscheidungen) bei einem Server-Log einer vielfrequentierten Website die Kosten und der Zeitaufwand der Identifizierung von Millionen von Einträgen eben diese Identifizierung praktisch unmöglich machen. Dass bei diesem Gedankenexperiment auch Dritte als „Steigbügelhalter" instrumentalisiert werden dürfen, ist dabei nur der nächste konsequente Schritt.

- Strafanzeige gegen Unbekannt

Für den Verantwortlichen ist auch dann eine namenlose Person identifizierbar, wenn die Zusammenführung von Datum und Person bei einem Dritten stattfinden bzw. die Zuordnungsinformation dort erzeugt werden kann. Es geht dementsprechend nicht nur um die „Mittel" des Verantwortlichen selbst – etwa die Zusammenführung verschiedener Datenbestände des Verantwortlichen –, sondern auch um den Einsatz eines Dritten als „Mittel". Dies kann die Menge der hypothetischen Szenarien der Zusammenführung von Daten und Person erheblich vergrößern, auch wenn in der Praxis – eng an den Gerichtsentscheidungen – in erster Linie die Frage erörtert wird, ob dem (nicht namentlich bekannten) Betroffenen die

Verübung einer Straftat gegen den Verantwortlichen vorgeworfen werden könnte. Ein Blick in die verschiedenen möglichen Straftaten des Haupt- und Nebenstrafrechts kann sich also auch datenschutzrechtlich lohnen, um die Staatsanwaltschaft als (fiktiven) „Identitätsbeschaffer" einsetzen zu können. Dass bei einer Strafanzeige, um an die Zusammenführung von Daten und Person zu gelangen, selbstverständlich das Risiko einer falschen Verdächtigung besteht, die ihrerseits strafbar ist (was wohl das „wahrscheinlich genutzte Mittel" auch illegal werden lässt), scheint dem Bundesgerichtshof nicht so wichtig gewesen zu sein. Er hat sich auf die kleine Teilmenge möglicher Fälle fokussiert, in denen tatsächlich der Verdacht besteht, dass von der IP-Adresse aus eine Straftat begangen wurde, nicht auf die Fälle, in denen die Strafanzeige nur erhoben wird, um an die Daten zu gelangen. Dann wäre aber konsequenterweise in allen anderen Fällen von anonymen Daten auszugehen und damit auch in dem konkret vom EuGH/BGH entschiedenen Fall zur dynamischen IP-Adresse, denn der Kläger – ein schleswig-holsteinischer Abgeordneter der Piraten-Partei – hatte selbst gar keinen „Anschlag" auf die Webseite verübt.

Wenn man dies weiterdenkt, kann das auch bedeuten, dass der Täter eines Diebstahls für das Opfer eine „identifizierbare Person" ist, selbst wenn das Opfer überhaupt nicht weiß, wer die Tat verübt hat. Die Schuhgröße des Täters, anhand eines am Tatort hinterlassenen Fußabdrucks für das Opfer ersichtlich, ist (in einer strukturierten Datensammlung) ein personenbezogenes Datum, wenn die Staatsanwaltschaft den Täter ermitteln und so dessen Person und Schuhgröße zusammenführen könnte, und zwar unabhängig davon, ob sie es auch tut.

Ungeachtet dessen kommen in der Theorie auch zivilrechtliche Auskunftsansprüche gegen einen Dritten, der über die Zuordnungsinformation verfügt, in Betracht – auch in Form vertraglicher Nebenansprüche. Überhaupt ist eine vertragliche Verbindung zwischen dem Verantwortlichen und dem Besitzer oder Beschaffer der Zuordnungsinformation kritisch, denn anhand dieser schuldrechtlichen Verbindung können ebenfalls Szenarien herbeikonstruiert werden. Der Phantasie zu den „wahrscheinlich genutzten Mitteln" sind kaum Grenzen gesetzt.

Ob dies alles zusammengenommen bedeutet, dass – wie manche Experten meinen und ähnlich wie dies die Datenschutzkonferenz ausführt (s. o.) – die Anonymisierung personenbezogener Daten heutzutage weitgehend eine Illusion ist, ist in diesem Kontext nicht entscheidend. Wichtig ist vielmehr: Wenn die Zuordnung zwischen Datum und Person tatsächlich hergestellt (und moniert) wird, wird die Frage, ob dies zeitlich davor wahrscheinlich war, in der Praxis keine Rolle mehr spielen. Denn nachher ist man immer schlauer. Deshalb wird das Ergebnis solcher Gedankenexperimente zu den „wahrscheinlich genutzten Mitteln" aus

Vorsichtsgründen häufig lauten, dass man auch dann, wenn man „nur“ im Besitz von IDs ist, trotzdem stets davon ausgehen muss, personenbezogene Daten in der Hand zu halten, obwohl man gar nicht weiß, wessen Daten das sind, und mit dem Betroffenen z. B. gar nicht in Kontakt treten kann.

- Gehashte Daten und MAC-Tracking

Vor diesem Hintergrund ein kleiner Exkurs zum Thema Hash-Werte und zur „Facebook-Customs-Audience“-Entscheidung des Verwaltungsgerichts Bayreuth vom Mai 2018, die vom Bayerischen Verwaltungsgerichtshof bestätigt wurde. Hash-Algorithmen bilden eine Art „lange Quersumme“ aus beliebigen Daten. Während die Quersumme leicht zu bilden ist, ist die Wiederherstellung der ursprünglichen Zahl bzw. Daten praktisch unmöglich. Beispielsweise ist sowohl die Quersumme von 14 als auch von 23 jeweils 5, sodass aus der Zahl 5 nicht gefolgert werden kann, ob ursprünglich die Zahl 14 oder 23 vorlag. Man kann „Hashing“ daher auch als eine Art Fingerabdruck eines Datensatzes beschreiben oder sogar als „Verschlüsselung ohne Entschlüsselungsmöglichkeit“. Wenn jemand einen Hash-Wert erhält und über die mutmaßlichen Ausgangsdaten verfügt, kann er feststellen, ob die Ausgangsdaten dem Absender des Hash-Wertes ebenfalls vorlagen oder nicht.

In der genannten Entscheidung ging es um den Abgleich von „gehashten“ E-Mail-Adressen. Ein Unternehmen hatte die Hash-Werte von E-Mail-Adressen von Werbekunden an Facebook gesandt und Facebook darum gebeten, gegenüber denjenigen Werbekunden, die Facebook ebenfalls „kennt“, zielgerichtet entsprechende Werbung zu schalten. Facebook glich also die übermittelten Hash-Werte mit den Hash-Werten ab, die aus den Facebook bekannten E-Mail-Adressen generiert worden waren, um Übereinstimmungen festzustellen. Waren die Hash-Werte identisch, wusste Facebook, dass es sich bei den E-Mail-Adressen, die dem Unternehmen vorlagen, um dieselben E-Mail-Adressen handelte, die auch Facebook vorlagen. Die nicht zuordenbaren E-Mail-Adressen kannte Facebook sowohl vor als auch nach dem Abgleich nicht, da Facebook aus deren Hash-Werten die ursprünglichen E-Mail-Adressen nicht „zurückrechnen“ konnte. Datenschutzrechtlich liegt in Bezug auf die übereinstimmenden Hash-Werte eine Übermittlung der personenbezogenen Daten des Betroffenen vor (da Facebook die Identität der Betroffenen kennt), während die übrigen Hash-Werte für Facebook anonyme Daten darstellen – was Facebook aber erst nach dem Abgleich weiß. Mit anderen Worten: Ein Teil der Hash-Werte weist für Facebook Personenbezug auf, ein anderer Teil nicht. Dementsprechend wurden zumindest auch personenbezogene Daten übermittelt, was aber – so die Gerichte, hier aber nicht weiter relevant – datenschutzrechtlich nicht zulässig war.

Auf dieser Basis beschäftigt sich nun das Bayerische Landesamt für Datenschutzaufsicht, das diese Entscheidungen erwirkt hat, in seinem Tätigkeitsbericht 2017/2018 mit dem sog. „Offline-Tracking", d. h. der Identifikation physischer Kunden in physischen Geschäften etwa anhand der MAC-Adressen der von ihnen mitgeführten Geräte:

„Zahlreiche Dienste zum Offline-Tracking sind derart ausgestaltet, dass die gehashten MAC-Adressen auf unbestimmte Zeit gespeichert und evtl. mit weiteren Daten zusammengeführt werden. Dies geschieht deshalb, weil Betreiber des Offline-Tracking meist davon ausgehen, es handle sich bei den gehashten Daten um anonymisierte Daten. Wir vertreten hierzu jedoch eine andere Auffassung: Bei der MAC-Adresse handelt es sich um ein personenbezogenes Datum, da hier die MAC-Adresse einem bestimmten Gerät zugeordnet ist und der Nutzer des Geräts mittelbar bestimmt werden kann. Zwar wird in der Regel die MAC-Adresse unter Verwendung eines Hash-Verfahrens verändert – das Hash-Verfahren führt jedoch nicht zu einer Anonymisierung der Daten. Diese Auffassung wurde durch einen Beschluss des Bayerischen Verwaltungsgerichtshofs vom 26. September 2018 bestätigt."

Diese „Extrapolation" der Gerichtsentscheidungen ist aus zweierlei Gründen fragwürdig. Zunächst ist zwar eine MAC-Adresse – im Gegensatz zu einer dynamisch durch einen Internet-Provider immer wieder neu vergebenen IP-Adresse – eine statische Adresse. Wer also weiß, wer das Gerät mit einer bestimmten MAC-Adresse verwendet, kann die MAC-Adresse – und die Daten, die von dieser oder an diese gesendet werden – der Person zuordnen. Für denjenigen aber, der nicht weiß, welcher Person die MAC-Adresse zuzuordnen ist, stellt sich gerade die Frage, ob es sich um eine für ihn identifizierbare Person handelt. Dafür muss – wenn einem nichts Besseres einfällt – das Beispiel der Staatsanwaltschaft bemüht werden: Dem Inhaber des Geräts mit der MAC-Adresse muss (aufgrund eines tatsächlichen Verdachts) eine Straftat vorgeworfen werden (s. o.). Schon dies schränkt die Fälle, in denen tatsächlich eine identifizierbare Person vorliegt, erheblich ein. Wie dann die Staatsanwaltschaft an die Zuordnung gelangt, erklärt das Bayerische Landesamt für Datenschutzaufsicht nicht. Einen Provider kann die Staatsanwaltschaft nicht fragen – MAC-Adressen werden nicht von einer zentralen Instanz „zugewiesen", sondern (unveränderlich) von den Herstellern der jeweiligen Hardware erzeugt –, d. h. die (forensische) Untersuchung wäre wesentlich aufwendiger.

Wird – unabhängig davon – ein Hash-Wert einer erhobenen MAC-Adresse ermittelt und die ursprüngliche MAC-Adresse gelöscht, kann die ursprüngliche MAC-Adresse nicht mehr „zurückgerechnet" werden. Man kann zwar sagen, dass für einen sehr kurzen Zeitraum die vollständige MAC-Adresse „verarbeitet" wurde, aber nach dem Löschen der ursprünglichen

MAC-Adresse ist diese Verarbeitung abgeschlossen. Das gilt nicht spezifisch für MAC-Adressen: Auch wer eine IP-Adresse erhebt und die letzten beiden Bytes kürzt (wie dies einige verfügbare Tracking-Verfahren vorsehen), hat für einen sehr kurzen Zeitraum – vor der Kürzung – die vollständige IP-Adresse „verarbeitet". Möglicherweise kann nach der Löschung der ursprünglichen MAC-Adresse der Inhaber des Geräts noch anderweitig ermittelt werden, aber die MAC-Adresse ist nicht mehr „bekannt".

Der Bayerische Verwaltungsgerichtshof hat auch nicht – wie vom Bayerischen Landesamt für Datenschutz behauptet – bestätigt, dass die Ermittlung eines Hash-Wertes nicht zu einer Anonymisierung von Daten führt, sondern, dass die Übermittlung von Hash-Werten (einer E-Mail-Adresse) an jemanden (Facebook), dem dieselbe E-Mail-Adresse schon vorlag (weil derjenige Inhaber eines Facebook-Accounts ist), eine Übermittlung von personenbezogenen Daten ist. Denn der Empfänger (Facebook) kann durch Bildung eines (eigenen) Hash-Wertes der ihm vorliegenden personenbezogenen Daten und Abgleich mit dem empfangenen Hash-Wert feststellen, dass es sich um dieselbe Person handelt, die der Absender bewerben will. Es liegt auf der Hand, dass dies nicht dasselbe ist wie die Generierung eines Hash-Wertes aus einer MAC-Adresse, die danach gelöscht wird.

Der Teufel liegt also, wie immer, im Detail.

- Anonymisierung

Unabhängig von all dem kann ein Verantwortlicher, der personenbezogene Daten verarbeitet und einer Löschpflicht unterliegt, ein Interesse daran haben, die Daten vom Personenbezug zu befreien, um sie weiter speichern zu können, weil sie dann nicht mehr dem Datenschutzrecht unterliegen. Letztlich stellt sich diese Frage auch jedem Arbeitgeber, wenn die Arbeitnehmer ausscheiden (s. unten Fall 33).

In einem von der österreichischen Datenschutzbehörde im Dezember 2018 entschiedenen Fall hatte das verantwortliche Unternehmen die Daten eines Betroffenen dadurch anonymisiert, dass sie dessen Stammdaten mit einem „Max Mustermann"-Datensatz überschrieben hatte. Damit waren zwar die verschiedenen mit der Person verknüpften Vorgangsdaten noch vorhanden, konnten aber keiner betroffenen Person mehr zugeordnet werden, sondern nur noch einem „Dummy". Die österreichische Datenschutzbehörde hielt die „endgültige" Anonymisierung durch Überschreiben mit den Dummy-Daten für eine „Löschung" im Sinne der DSGVO. Eine Löschung müsse nicht unbedingt bedeuten, dass die Daten für alle Zeiten irreversibel keiner Person mehr zugeordnet werden können. Eine mögliche künftige Rekon-

struierbarkeit anhand neuer technischer Mittel (oder neuer Datenbestände) mache die „Löschung durch Unkenntlichmachung“ nicht unzureichend. Damit würde die Anonymisierung eine veritable Alternative zur Löschung, wenn man den Informationsgehalt der Daten (mit Ausnahme des Personenbezugs) noch irgendwie weiterhin konservieren möchte (Stichwort „big data“).

Ebenso sieht dies auch der Europäische Datenschutzausschuss in seinen Empfehlungen vom November 2019 zum Thema „*privacy by design / by default*“:

„Anonymization of personal data is an alternative to deletion, provided that all the relevant contextual elements are taken into account and the likelihood and severity of the risk, including the risk of re-identification, is regularly assessed.“

Nun könnte man aber gleichwohl wieder die Entscheidungen zur dynamischen IP-Adresse heranziehen. Das verantwortliche Unternehmen könnte nach der vermeintlichen Anonymisierung feststellen, dass der Betroffene eine Straftat gegen das Unternehmen begangen hat, kann aber den Täter nicht mehr namentlich benennen. Vielleicht kann die Staatsanwaltschaft mit ihren Mitteln die Identität aufklären? Wenn dies möglich erscheint, würde es sich weiterhin um personenbezogene Daten handeln – egal, wie viele Betroffene das betrifft, egal, ob der Betroffene tatsächlich eine Straftat begangen hat oder nicht (s. o.).

Diese Erkenntnis kann dazu führen, dass eine sichere Anonymisierung – also jedweder Ausschluss eines Personenbezuges – nur durch zwei Wege erreicht werden kann: Entweder die Daten werden (endgültig) aggregiert, sprich „verstümmelt“. Wenn eine Datenbank nur noch die Information enthält, dass 47 Personen in der Datenbank Schuhgröße 43 haben, kann weder die Zuordnungsinformation für die einzelne Person ermittelt werden noch – in der Folge – deren Identität. In diesem Zusammenhang hat der Datenschutzbeauftragte für Baden-Württemberg in seinem Ratgeber für Beschäftigtendatenschutz empfohlen, bei anonymen Mitarbeiterbefragungen auf eine Auswertung zu verzichten, wenn die (vermeintlich) anonymen Daten auf weniger als sieben Personen zurückzuführen sind. Denn bei einer geringeren Anzahl von Betroffenen könne eine Zuordnung grundsätzlich möglich sein, auch wenn vermeintlich anonyme Daten verarbeitet werden.

Oder die Einträge werden verwürfelt, also zufällig neu zusammengesetzt. Dies hat den Vorteil, dass die Daten unter Umständen „statistisch korrekt“ bleiben, aber Einzelfälle nicht mehr rekonstruierbar sind. Dies führt zur sogenannten „*differential privacy*“, die von Wikipedia wie folgt definiert wird:

„Differential Privacy (engl. für ‚differentielle Privatsphäre') hat das Ziel, die Genauigkeit von Antworten zu Anfragen an Datenbanken zu maximieren, unter Minimierung der Wahrscheinlichkeit, die zur Beantwortung verwendeten Datensätze identifizieren zu können. Der Begriff fällt in den Bereich des sicheren, Privatsphären erhaltenden Veröffentlichens von sensiblen Informationen. Mechanismen, die Differential Privacy erfüllen, verhindern, dass Angreifer unterscheiden können, ob eine bestimmte Person in einer Datenbank enthalten ist oder nicht."

Was demgegenüber nicht so einfach funktioniert, ist, einfach eine Zuordnungsinformation zu löschen, sodass nicht mehr nachvollzogen werden kann, wer „1234" ist. Schon mit internen Mitteln des Verantwortlichen ist die Identität manchmal bestimmbar, mit den Mitteln eines „instrumentalisierten" Dritten häufiger.

- Identifizierbarkeit als „on/off"-Problematik

Der – an dieser Stelle fast schon vergessene – Ausgangsfall enthält in diesem Kontext eine weitere Wendung im Dickicht der Anonymisierung, die in der datenintensiven Praxis bedacht werden muss. Erhält der Verantwortliche, selbst wenn er die Zuordnungsinformation gelöscht hat, zu einem späteren Zeitpunkt neue Daten, die in der Gesamtschau den Personenbezug wieder herstellen lassen, so führt dies dazu, dass auch der Schutz des Datenschutzrechts wieder auflebt. Die Daten können im Zeitraum bis dahin durchaus anonym gewesen sein. Aber häufig wird der Verantwortliche das Hinzutreten neuer Zuordnungsinformationen gar nicht bemerken, zumal in komplexeren Organisationen. Es genügt, dass er zu einem späteren Zeitpunkt (wieder) in die Lage versetzt wird, durch das Zusammenführen von Datenbeständen – die Aufsichtsbehörden sprechen von „Verkettung" – den Personenbezug wieder herzustellen, und dass die dafür erforderlichen Mittel *„nach allgemeinem Ermessen wahrscheinlich genutzt werden"*. Dabei sind – nach Erwägungsgrund 26 – die Kosten, der Zeitaufwand, die verfügbare Technologie und die technologischen Entwicklungen zu berücksichtigen.

Im Ausgangsfall könnten die Daten im „data lake" der Huber AG mit den Kundendaten der Maier GmbH verknüpft werden und mit großer Wahrscheinlichkeit verschiedene Kunden der Huber AG re-identifiziert werden. Hat beispielsweise ein Kaufmann, der ein Ladengeschäft für Bett- und Unterwäsche betreibt, sowohl bei der Huber AG als auch bei der Maier GmbH Ware in bestimmtem Umfang geordert, wird sein Gesamt-„Profil" in beiden Datenmengen sehr ähnlich sein. Die Zuordnung seiner Identität, die mit den Daten der Maier GmbH möglich ist, kann dann auch auf die entsprechenden Daten der Huber AG übertragen

werden. Die dafür notwendigen Mittel sind heutzutage für jedes Unternehmen, das einen „data lake“ betreibt, „in Reichweite“.

Zwar greift die DSGVO insgesamt nur dann ein, wenn personenbezogene Daten irgendwie tatsächlich als solche „verarbeitet“ werden, aber auf eine explizite Kenntnis des bestehenden Personenbezugs aufseiten des Verantwortlichen kommt es nicht an. Jeder Zugriff bzw. jede „Umspeicherung“ der entsprechenden Daten der Huber AG und/oder der Maier GmbH stellt eine datenschutzrechtlich relevante Verarbeitungshandlung dar, und zwar unabhängig davon, ob der Huber AG (bzw. ihren Mitarbeitern) dies „bewusst“ ist, und unabhängig davon, ob sie von den verfügbaren Mitteln zur Re-Identifizierung Gebrauch macht. Die Identifizierbarkeit der natürlichen Person ist ein „on/off“-Kriterium, auf dessen Vorliegen die Anwendbarkeit des gesamten Datenschutzrechts beruht, und kein „Graukeil“ im Sinne eines gleitenden Maßstabes.

Wenn man den Fall abstrahiert, müssten Verantwortliche beständig Datenmengen, deren Anonymität sie unterstellen, anhand sämtlicher ihnen sonst zur Verfügung stehender Daten daraufhin überprüfen, ob ihnen nicht eine De-Anonymisierung der für anonym gehaltenen Daten möglich ist und damit die Schwelle zur Identifizierbarkeit „gerade so“ überschritten wurde. In diesem Fall muss der Verantwortliche die „nicht mehr anonymen“, also nun (wieder) personenbezogenen Daten entsprechend behandeln – mit allen datenschutzrechtlichen Konsequenzen wie Pflichtinformationen nach der Re-Identifizierung, Bestimmung der Legitimationsgrundlage, Anwendung risikoangemessener technischer und organisatorischer Maßnahmen, Einhaltung der „*privacy by design*“-Vorgaben, ggf. Durchführung einer Datenschutz-Folgenabschätzung, ggf. Abschluss einer Auftragsverarbeitungsvereinbarung mit Dritten und dergleichen mehr. Es ist auch offen, welche Anstrengungen in diesem Fall unternommen werden müssen, um den Betroffenen „zu Ende zu identifizieren“, etwa um diesen informieren oder seine Einwilligung einholen zu können. Eigentlich ergibt sich aus Art. 11 DSGVO, dass der Verantwortliche nicht zu einer „Zu-Ende-Identifizierung“, nur um Betroffenenrechte wahren zu können, verpflichtet ist. Denn diese würde nur zur Erhebung von noch mehr personenbezogenen Daten einzig zum Zweck der Einhaltung der DSGVO führen, was der Gesetzgeber nicht gutheißen wollte (s. auch unten Fall 39). Die entscheidende Frage hierbei wird aber sein, ob nicht der Verantwortliche schon alle relevanten Informationen hat, also nur „richtig danach suchen“ muss, oder ob er zusätzliche Informationen von Dritten einholen muss („Identitätsrecherche“). Nur letzteres wollte der Gesetzgeber dem Verantwortlichen erlassen.

Insbesondere in größeren Unternehmen dürfte diese Aufgabe des permanenten Abgleichs und der Folgen bei der „Entdeckung neuer personenbezogener Daten“ kaum mit überschaubaren Mitteln und in praktikablen (zu dokumentierenden!) Prozessen zu bewältigen sein. Hinzu kommt auch noch die laufende Überwachung der Frage, welche neuen Technologien sich etabliert haben, deren Anwendung „wahrscheinlich“ geworden ist. Nur am Rande sei in diesem Zusammenhang darauf hingewiesen, dass der Europäische Datenschutzausschuss in Empfehlungen vom November 2019 zum Thema *„privacy by design / by default“* das ständige Monitoring der Weiterentwicklung des *„state of the art“* sowohl bei technischen als auch bei organisatorischen Maßnahmen hervorgehoben hat:

„the reference to “state of the art” imposes an obligation on controllers, when determining the appropriate technical and organisational measures, to take account of the current progress in technology that is available in the market. This means that controllers must have knowledge of and stay up to date on technological advances, how technology can present data protection risks to the processing operation, and how to implement the measures and safeguards that secure effective implementation of the principles and rights of data subjects in face of the technological landscape. [...] The “state of the art” criterion does not only apply to technological measures, but also to organisational ones. Lack of adequate organisational measures can lower or even completely undermine the effectiveness of a chosen technology.“

Ob ungeachtet dessen eine (öffentliche?) „Selbstverpflichtung“ des Verantwortlichen, keine Re-Identifizierung zu betreiben, selbst wenn er das könnte, hilft, ist offen. Dem Verantwortlichen bliebe damit nur der („sichere“) Ausweg, selbst für anonym gehaltene Daten „wie“ personenbezogene Daten zu behandeln. Dass dadurch der begriffliche Anspruch der DSGVO, „nur“ personenbezogene Daten zu regulieren, in sein Gegenteil verkehrt wird, und der Anwendungsbereich der komplementären EU-Verordnung „über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union“ noch weiter schrumpft, ist da nur eine Petitesse.

➢ Einen hab‘ ich noch!

Wer an dieser Stelle von der Komplexität des Themas noch nicht genug hat, der kann sich mit einer weiteren Windung auseinandersetzen: Nach Ansicht der Art.-29-Datenschutzgruppe in ihrem Working Paper 216 (2014) ist die Anonymisierung personenbezogener Daten als solche – als „Schritt aus dem Datenschutzrecht“ – eine Verarbeitungshandlung, die datenschutzrechtlich legitimiert sein muss. Da die Anonymisierung unter diesem Blickwin-

kel meist eine Zweckänderung darstellen wird, muss also der Betroffene von der bevorstehenden Anonymisierung durch eine Zweckänderungsmitteilung in Kenntnis gesetzt werden. Ist die Anonymisierung als Verarbeitungshandlung nicht mit dem ursprünglichen Zweck kompatibel, muss eine Legitimationsgrundlage für die Anonymisierung geschaffen werden. Bei Anonymisierung von Daten mit hohem Risiko muss eine Datenschutz-Folgenabschätzung durchgeführt werden. Von der österreichischen Datenschutzbehörde wurde diese – von Juristen als „absurd" und praxisfern bezeichnete – Theorie im oben aufgeführten Fall nicht thematisiert.

Nach der sog. „DSFA-Muss-Liste" („blacklist"), die Fälle auflistet, in denen in jedem Fall eine Datenschutz-Folgenabschätzung durchzuführen ist (Art. 35 Abs. 4 DSGVO), findet sich unter Ziff. 15 der Eintrag:

„Anonymisierung von besonderen personenbezogenen Daten nach Artikel 9 DS-GVO nicht nur in Einzelfällen (in Bezug auf die Zahl der betroffenen Personen und die Angaben je betroffener Person) zum Zweck der Übermittlung an Dritte".

Als Beispiel wird angegeben:

„Umfangreiche besondere personenbezogene Daten werden durch ein Apothekenrechenzentrum oder eine Versicherung anonymisiert und zu anderen Zwecken selbst verarbeitet oder an Dritte weitergegeben."

Hier ist sogar beim „Schritt aus dem Datenschutzrecht" erhöhter Aufwand im Vorfeld in Gestalt einer Datenschutz-Folgenabschätzung – obwohl die Daten danach gar nicht mehr dem Datenschutzrecht unterliegen – zu betreiben. Es kann nur vermutet werden, dass die Motivation der Datenschutzbehörden hier darin lag, dem Verantwortlichen eine besondere Prüfpflicht als Warnung aufzuerlegen, damit dieser sich vertieft mit der Frage beschäftigt, ob die Anonymisierung auch wirklich zu anonymen Daten führt.

Es wird also spannend, wenn erstmals ein Betroffener gegen eine Anonymisierung seiner Daten mit der Begründung vorgeht, man habe ihn davon nicht in Kenntnis gesetzt und es mangele an einer Legitimationsgrundlage. Oder eine Behörde die Anonymisierung aus diesen Gründen kritisiert und ein Bußgeld verhängt. Beides nicht sehr wahrscheinlich? Man wird sehen.

Fall 33:
Der löscht einfach alles

Praktischer Fall: Herr Maier ist Geschäftsführer der Huber GmbH. Sein Geschäftsführer-Anstellungsvertrag wird von der Gesellschafterversammlung fristgerecht ordentlich gekündigt. Am letzten Tag der Kündigungsfrist löscht Herr Maier sämtliche E-Mails von und an sich, die er in seinem Postfach noch vorfindet und die bislang nicht – z. B. wegen steuerrechtlicher Aufbewahrungspflichten – in einem Archivsystem der Huber GmbH erfasst wurden. Sein Nachfolger, Herr Müller, der zwei Tage davor zum Unternehmen stieß, sucht nach dem Weggang von Herrn Maier nach E-Mails zu einem bestimmten Vorgang.

Dieser Fall schließt thematisch an Fall 4 oben an. Dort ging es um den Auskunftsanspruch eines Beschäftigten im Zusammenhang mit dessen Bewegungsdaten, hier dagegen geht es um die Umsetzung eines Löschanspruchs eines Geschäftsführers – dessen Anstellungsvertrag wohl nicht der Regelung des § 26 BDSG zum Beschäftigtendatenschutz unterfällt – im Wege einer „datenschutzrechtlichen Selbsthilfe". Für Bewegungsdaten von Beschäftigten wird das Thema noch weiter unten im Rahmen eines Exkurses angeschnitten.

Die im Fallbeispiel vielleicht etwas ungewöhnliche Form der „Exekution" durch Löschen der eigenen Bewegungsdaten wirft natürlich zunächst einmal die vorgelagerte Frage auf: Hätte die Korrespondenz von und an Herrn Maier, wenn er das Unternehmen ohne zu löschen verlassen, aber sogleich die Löschung (Art. 17 DSGVO) verlangt hätte, ohnehin gelöscht werden müssen? Gesetzt den Fall, gesetzliche Aufbewahrungspflichten wären nicht einschlägig, darf das Unternehmen sämtliche unternehmensbezogene Kommunikation nach dem Austritt des Mitarbeiters „behalten", eben weil sie „Unternehmenskommunikation" darstellt? Zweifellos sind die E-Mails im Postfach von Herrn Maier personenbezogene Daten und zweifellos ist Herr Maier einer der Betroffenen – neben anderen Personen wie dem jeweiligen Absender bzw. Empfänger oder sonstigen Personen, die in der jeweiligen E-Mail eine Rolle spielen.

➢ Datenschutzrechtliche Legitimationsgrundlage für Bewegungsdaten

Die Kernfrage ist, auf welche Legitimationsgrundlage für das „Behaltendürfen" der E-Mails sich die Huber GmbH nach dem Ausscheiden von Herrn Maier stützen kann. Eine Einwilligung scheidet aus, wenn Herr Maier diese nicht erklärt. Ohnehin könnte er eine frühere Einwilligung – vorausgesetzt, die wäre freiwillig gewesen (ansonsten wäre sie unwirksam gewesen) – jederzeit widerrufen.

Ob die personenbezogenen Daten nach dem Ende des Geschäftsführer-Anstellungsvertrages immer noch „irgendwie“ für die Durchführung eben dieses Vertrages „erforderlich“ sind, dürfte zweifelhaft sein. Der Umstand, dass für einen Geschäftsführer wohl nicht die Regelung des § 26 BDSG, sondern die allgemeine Legitimationsgrundlage „Vertrag“ der DSGVO (hier in Gestalt des Geschäftsführer-Anstellungsvertrages) einschlägige Legitimationsgrundlage ist, kann keinen entscheidenden Unterschied machen. Man könnte in Richtung einer fortlaufenden Erforderlichkeit argumentieren, wenn man eine nachlaufende vertragliche Pflicht anerkennen würde, dem Dienst- oder Arbeitgeber seine „Arbeitsergebnisse“ – hier in Form von E-Mails – dauerhaft zu überlassen (Dokumentationspflicht). Dabei sind im hiesigen Sachverhalt im Grundsatz auch Organpflichten zur zweckentsprechenden Organisation eines – unternehmensnotwendigen – „Wissensmanagements“ in der GmbH (§ 43 GmbHG) zu berücksichtigen: Eigentlich hat der Geschäftsführer die (Organ-)Pflicht, dafür zu sorgen, dass unternehmensbezogener E-Mail-Verkehr der Gesellschaft (so lange wie irgend möglich) zur Verfügung steht. Allerdings wird unter der DSGVO kaum eine (woher auch immer stammende) „Verpflichtung zur Erteilung bzw. zum Nichtwiderruf einer Einwilligung“ akzeptiert werden können. Man könnte aber daran denken, die Einwilligung in die weitere Aufbewahrung bei der Gesellschaft als vertragliche Gegenleistung definieren, die mit der Vergütung abgegolten wird (s. dazu auch oben Fall 30).

Was (ungeschriebene) Nebenpflichten eines Geschäftsführer-Anstellungsvertrages anbelangt, werden in Gerichtsentscheidungen und in der Kommentarliteratur – unter dem Titel nachlaufender (Treue-)Pflichten – eher Verschwiegenheitspflichten und Wettbewerbsverbote behandelt. In der Vergangenheit ist man wohl wie selbstverständlich davon ausgegangen, dass die Arbeitsergebnisse dem Arbeit- bzw. Dienstgeber „gehören“. Die Annahme einer allgemeinen (nachlaufenden Vertrags-)„Pflicht, der Gesellschaft seine Arbeitsergebnisse dauerhaft zu überlassen“, dürfte auch vor dem Hintergrund einer sich abzeichnenden „vertraglichen Inhaltskontrolle“ und der datenschutzrechtlichen Grundprinzipien schwer zu rechtfertigen sein (vgl. dazu auch oben Fall 30). Nur in einem Fall hat der Gesetzgeber die Kollision von (satzungsgemäßer oder vertraglicher) Aufbewahrungspflicht und (datenschutzrechtlicher) Löschpflicht in der Person des Organs einer Gesellschaft explizit geregelt und dabei der Aufbewahrungspflicht den Vorzug gegeben (§ 35 Abs. 3 BDSG), was (natürlich) auch bereits als europarechtswidrig (weil nicht DSGVO-konform) bezeichnet wurde. Ein – mit dem Risiko einer europarechtswidrigen Legitimationsgrundlage versehener – Ausweg wäre also für Bewegungsdaten (sowohl der Geschäftsführer als auch der Beschäftigten) die Statuierung einer satzungsmäßigen Aufbewahrungspflicht, die dann einer Löschpflicht vorgehen würde.

➢ Interessenabwägung nach Ende des Anstellungsvertrages?

Ansonsten bliebe noch die Interessenabwägung. Wahrscheinlich wird hierbei zunächst eine Zweckänderung vorliegen: Ursprünglicher Zweck war der Anstellungsvertrag (d. h. das Vertragsverhältnis), nun basiert der Zweck auf dem Interesse des Unternehmens, betriebliche Kommunikation zu betrieblichen Zwecken nach dem Vertragsende verfügbar zu halten (s. oben Fall 17). Auch wenn hier wohl von Zweckkompatibilität auszugehen ist, müsste Herr Maier bei seinem Ausscheiden eine Zweckänderungs-Pflichtinformation erhalten. Er könnte dann immer noch dieser Interessenabwägung widersprechen, wenn man nicht davon ausgeht, dass die Zweckkompatibilität auf Basis des ursprünglichen Zwecks den Folge-Legitimationsgrund ersetzt (s. oben Fall 5). Dies darf er nach Art. 21 Abs. 1 DSGVO zwar nur *„aus Gründen, die sich aus seiner besonderen Situation ergeben“*, d. h. die im Rahmen einer typisierten Interessenabwägung nicht ohnehin zu berücksichtigen waren (s. oben Fall 26). Herr Maier könnte aber etwa behaupten, dass er das Unternehmen im Unfrieden verlassen habe und nicht möchte, dass dort mit seiner Korrespondenz „Schindluder“ betrieben wird. Ob ein Gericht dies als „wirksamen“ Widerspruch anerkennen würde, ist allerdings fraglich.

Geht man davon aus, dass Herr Maier einen solchen besonderen Grund ins Feld führen könnte, so dürfte die Huber GmbH die Kommunikationen nur noch weiter verarbeiten, wenn sie *„zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen“*, oder wenn die Verarbeitung der Kommunikationen *„der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient“* (Art. 21 Abs. 1 DSGVO). Dies wird dann für jede einzelne Kommunikation gesondert zu beurteilen sein. Wie immer gilt: Die mustergültige Erfüllung der DSGVO lässt sich beliebig komplex gestalten und führt dann zu beliebig hohem Aufwand (s. dazu schon oben Fall 14).

➢ „Dateneigentum“ des Arbeitgebers?

Man sieht, dass (nicht nur) hier eine „außerrechtliche“ Vorstellung von einem „Dateneigentum“ (der Huber GmbH gehören „ihre“ Daten) und das Datenschutzrecht kollidieren. Da es ohnehin kaum mehr Daten ohne Personenbezug gibt (s. oben Fall 15), stellt im Grunde schon die DSGVO selbst die neue „Eigentumsordnung“ an Daten dar. Entsprechend dem Grundgedanken einer Treuhand bzw. eines Eigentümer-Besitzer-Verhältnisses ist – aus der Perspektive zivilrechtlicher Kategorien sinnbildlich gesehen – der Betroffene der „Eigentümer“ der Daten, während der Verantwortliche (im Sinne des Datenschutzrechts) nur deren

„Besitzer“ ist. Solange er „rechtmäßig besitzt“ – also eine datenschutzrechtliche Legitimationsgrundlage für die Verarbeitung besteht – darf er die Daten im Rahmen der Zweckbindung verarbeiten. Solcher rechtmäßiger (legitimierter) Besitz kann im Bereich der Interessenabwägung – sprich: der mutmaßlichen Einwilligung auf Basis typisierter (bzw. antizipierter) Interessen des Betroffenen – auch gegen den Willen des Eigentümers (Betroffenen) bestehen, denn das Widerspruchsrecht des Art. 21 DSGVO besteht nur im Rahmen der Direktwerbung und ansonsten nur dann, wenn *„Gründe, die sich aus seiner besonderen Situation ergeben“*, vorliegen. Liegen die Voraussetzungen des Art. 21 DSGVO nicht vor und ist die Legitimationsgrundlage Interessenabwägung noch gegeben, kann der Betroffene die Verarbeitung nicht verhindern, selbst wenn er mit der Verarbeitung nicht einverstanden ist (aber eben vom Verantwortlichen nicht gefragt werden musste; s. aber zur Frage, wann er gefragt werden muss, oben Fall 17).

Wenn jedoch die Verarbeitung, insbesondere aber die Speicherung, nicht mehr auf eine datenschutzrechtliche Legitimationsgrundlage gestützt werden kann, wird der Verantwortliche zum „unrechtmäßigen Besitzer“. Der unrechtmäßige Besitzer muss den Besitz an den Eigentümer herausgeben, also – in der „Sprache der Datenschützer“ – löschen (s. aber im Detail dazu oben Fall 28). Auch während der Trennung von Eigentum und Besitz ist der Besitzer – wie ein Treuhänder – dem Eigentümer immer Rechenschaft über die Verarbeitung schuldig (Auskunftsanspruch etc.).

Es liegt daher auf der Hand, dass es keiner (weiteren) Regulierung eines Dateneigentums mehr bedarf, wenn man das Datenschutzrecht als „Ersatz-Eigentumsordnung für Daten“ ansieht. Diesen umfassenden Anspruch trägt die DSGVO bereits in Erwägungsgrund 7 in sich („Natürliche Personen sollten die Kontrolle über ihre eigenen Daten besitzen“). Unter solchen Vorgaben kann kein Eigentum an den Daten frei übertragen werden (im Sinne einer Eigentumsübertragung im „klassischen“ sachenrechtlichen Sinne): Gerade die Freigabe solcher Transaktionen durch den Betroffenen in Form der Einwilligung ist jederzeit widerruflich. Dies läuft dem (faktischen) Zweck vieler Daten, Wirtschaftsgut zu sein und als solches in Märkten oder Unternehmen zirkulieren zu können, eigentlich zuwider. Deshalb wird in regelmäßigen Abständen immer wieder nach einer separaten Regulierung eines „Dateneigentums“ gerufen, das außerhalb des Datenschutzrechts, des Urheberrechts und was sonst noch so alles rechtliche Verhältnisse an Informationen regelt, zur Anwendung kommen soll. Allerdings bleibt da gar nicht mehr so viel übrig, was sich noch regeln ließe – die Luft ist durch die DSGVO sehr dünn geworden.

Eine naheliegende Erweiterung dieses Falles ist übrigens ein von Herrn Maier erlaubtermaßen gemischt privat-betrieblich genutzter E-Mail-Account, in den sein Nachfolger hineinsehen möchte. Die sich hierbei ergebenden Fragen im Hinblick auf das Fernmeldegeheimnis sind oben in Fall 31 skizziert. Würde Herr Maier die Genehmigung verweigern, dass Einblick in seinen E-Mail-Account genommen wird, würde diese Konstellation derzeit kaum rechtssicher zu lösen sein.

➢ Exkurs: Beschäftigtendatenschutz

Eine weitere interessante Frage ist, wann die Bewegungsdaten eines Beschäftigten – also im Anwendungsbereich des § 26 BDSG und nicht, wie in der obigen Fallkonstellation, eines Geschäftsführers – nach dessen Ausscheiden aus dem Unternehmen zu löschen sind. An sich endet die Legitimationsgrundlage des § 26 BDSG mit dem Ausscheiden des Mitarbeiters: Das Anstellungsverhältnis ist beendet. Damit ist auch die Legitimationsgrundlage für die Verarbeitung der unternehmensbezogenen Kontaktdaten eigentlich entfallen und diese sind zu löschen (s. oben Fall 1). Ob § 26 BDSG insoweit eine „Nachlaufwirkung" nach dem Ende des Anstellungsverhältnisses entfaltet, wurde auch für Beschäftigte noch nicht im Detail erörtert. Dies hängt damit zusammen, dass unter „Beschäftigtendaten" rechtlich häufig nur bzw. in erster Linie Personalaktendaten verstanden werden. Zu Personalaktendaten hat das Landesarbeitsgericht Sachsen-Anhalt in einer Entscheidung vom November 2018 unter dem Blickwinkel eines DSGVO-Löschanspruchs bezüglich einer Abmahnung in einer Personalakte geurteilt, dass jedenfalls nach Beendigung des Beschäftigungsverhältnisses der Zweck der Abmahnung (Warnfunktion) nicht mehr zum Tragen komme. Das personenbezogene Datum der Abmahnung war damit *„für die Zwecke, für die es [...] verarbeitet wurde, nicht mehr notwendig"*. Das Landesarbeitsgericht verwies hier auf Art. 17 Abs. 1 lit. a DSGVO, berief sich aber in der Sache auf den Wegfall des Legitimationsgrundes von § 26 BDSG (bzw. Art. 6 Abs. 1 S. 1 lit. b DSGVO). Die Entscheidung spricht auf Ebene der Granularität auch dafür, dass die Personalakte hinsichtlich des datenschutzrechtlich relevanten Löschzeitpunkts nicht als „ein Dokument" betrachtet werden sollte. Aber wie gesagt, gibt dies eher wenig für die Situation in Bezug auf Bewegungsdaten her.

Mutmaßlich verhält es sich für Bewegungsdaten von Beschäftigten ähnlich wie oben für den Geschäftsführer skizziert: Es liegt eine Zweckänderung vor, die neue Legitimationsgrundlage ist eine Interessenabwägung, der Betroffene muss eine Zweckänderungsmitteilung erhalten und kann in begründeten Ausnahmefällen Widerspruch gegen die weitere Verarbeitung einlegen.

Dabei wird man in der Praxis – um noch eine weitere Datenkategorie mit einzubeziehen – auch feststellen, dass sich häufig unternehmensbezogene Kontaktdaten und Bewegungsdaten kaum voneinander trennen lassen. Insbesondere in der internen und externen Kommunikation dienen die unternehmensbezogenen Kontaktdaten, allem voran die E-Mail-Adresse, der Adressierung von Bewegungsdaten, die der Beschäftigte an jemanden geschrieben oder von jemandem erhalten hat. Eine E-Mail enthält demnach beispielsweise immer beide Kategorien von Daten (unternehmensbezogene Kontaktdaten und Bewegungsdaten des Beschäftigten). Eine isolierte Löschung der unternehmensbezogenen Kontaktdaten – also beispielsweise die Schwärzung der E-Mail-Adresse in einer Mail – wird die E-Mail (also die Bewegungsdaten) häufig nicht wirksam anonymisieren, und zwar auch deshalb, weil der Inhalt eines Dokuments (E-Mail, Aktenvermerk etc.) häufig selbst dann noch eine Zuordnung zu einem bestimmten Mitarbeiter zulässt (zumindest für die ermittelnde Staatsanwaltschaft, wenn dem Mitarbeiter eine Straftat vorgeworfen werden würde, s. dazu oben Fall 32).

Wie lange ist nun aber die zulässige Speicherdauer – darf der Arbeitgeber, vorausgesetzt, der Betroffene erhebt keinen wirksamen Widerspruch, die unternehmensbezogenen Kontaktdaten und die Bewegungsdaten des vormaligen Beschäftigten „ewig" weiter speichern? Verliert das Interesse des Arbeitgebers über den Verlauf der Zeit hinweg an Wert (s. dazu oben Fall 8)?

Solange ein Mitarbeiter noch im Unternehmen befindlich ist, für unternehmensinterne (Ursachen-) Befragungen noch zur Verfügung steht und das Beschäftigungsverhältnis noch eine taugliche „Behaltensgrundlage" hinsichtlich der (Bewegungs-) Daten darstellt, wird man dem verantwortlichen Arbeitgeber wohl eine gewisse „Dispositionsbefugnis" über die Bewegungsdaten im Rahmen der betrieblichen Notwendigkeiten zubilligen müssen. Was also aufzubewahren „erforderlich" ist, kann der Arbeitgeber aufgrund der Strukturierung seiner betrieblichen Abläufe ein gutes Stück weit selbst bestimmen. Allerdings werden auch hier E-Mails wie „Komme heute erst um 13 Uhr zum Mittagessen, weil ich vorher zum Arzt muss" vom Verantwortlichen nicht bis zum Ende des Beschäftigungsverhältnisses oder gar darüber hinaus aufbewahrt werden dürfen, weil der (vom Inhalt der E-Mail gekennzeichnete) Zweck noch am Tag des Verfassens der E-Mail entfällt (Art. 17 Abs. 1 lit. a) DSGVO). Dies ist die zwangsläufige Folge der vom Gesetzgeber (wohl) intendierten und von den Datenschutzaufsichtsbehörden stets wiederholten „Einzelfallbetrachtung" jedes personenbezogenen Datums (s. zur Einzelfallbetrachtung auch oben Fall 26). In diese Richtung geht auch die oben erwähnte Entscheidung des Landesarbeitsgerichts Sachsen-Anhalt.

Scheidet der Mitarbeiter aus und hinterlässt jede Menge innerbetriebliche Kommunikation, so würde man wohl an gesetzliche Aufbewahrungspflichten, etwa aus dem Bereich des Steuer- oder Handelsrechts, denken. Aber ist es aus diesem Blickwinkel entscheidend, welcher Mitarbeiter z. B. einen Buchungssatz angelegt oder verändert hat, wenn dieser Mitarbeiter nicht mehr im Unternehmen tätig ist? Der Steuerpflichtige ist in aller Regel das Unternehmen, nicht ein individueller Mitarbeiter. Für die Finanzverwaltung oder den Jahresabschlussprüfer ist im Grunde nicht erheblich, welcher ausgeschiedene Mitarbeiter etwas getan oder veranlasst hat, sondern dass dies „vom Unternehmen" getan oder veranlasst wurde. Wenn überhaupt, wird die Finanzverwaltung im Rahmen einer Betriebsprüfung das Unternehmen auffordern, bestimmte Umstände zu klären, und für das Unternehmen wird im Regelfall der „Rückgriff" auf ausgeschiedene Mitarbeiter aus faktischen oder rechtlichen Gründen ausscheiden. Aus datenschutzrechtlicher Perspektive wird daher die Aufbewahrungspflicht kaum an die Identität ausgeschiedener Mitarbeiter anknüpfen. Es besteht also die „Gefahr", dass auch insoweit anonymisierte Daten die steuer- und handelsrechtlichen Zwecke erfüllen. Es wäre interessant, die Reaktion eines Betriebsprüfers zu sehen, wenn auf einer Rechnung des Unternehmens der eigene Sachbearbeiter (der nicht zu den Pflichtangaben im Sinne von § 14 Abs. 4 UStG gehört) geschwärzt wäre mit dem Hinweis, dass dieser Sachbearbeiter das Unternehmen verlassen hat und dessen Daten zu löschen waren. Zur Abrundung sei hier aber auch noch einmal auf das Thema „satzungsmäßige Aufbewahrungspflichten" (§ 35 Abs. 3 BDSG) hingewiesen (s. o.).

Würde man sowohl für unternehmensbezogene Kontaktdaten als auch für Bewegungsdaten von einer „nachlaufenden Interessenabwägung" im Anschluss an das Beschäftigungsverhältnis und aufgrund der überragenden betrieblichen Interessen des Arbeitgebers von einer üppigen Dauer dieses Legitimationsgrundes ausgehen, so kommt doch auch die längste Frist irgendwann an ihr Ende (s. im Grundsatz schon Fall 8 oben). Dabei ist auch zu berücksichtigen, dass bei einer Fortspeicherung zu Nachweiszwecken im Kontext möglicher (prozessualer) Auseinandersetzungen über Verantwortlichkeiten (Art. 17 Abs. 3 lit. e DSGVO) eine solche Auseinandersetzung konkret drohen muss – eine nur abstrakte Gefahr (Stichwort Verjährungsfristen) ist zu wenig (s. dazu oben Fall 14). Auch wenn die abstrakte Gefahr das „Interesse" des Arbeitgebers nicht ausschließt, ist diese Wertung geeignet, ein solches „Interesse" im Rahmen einer Interessenabwägung zeitlich zu beschränken. Selbst innerhalb der Verjährungsfristen von möglichen Regressansprüchen gegen einzelne Beschäftigte – für die der Arbeitgeber nachweisen muss, dass der Beschäftigte gegen Pflichten verstoßen hat, und daher möglicherweise protokollierte Bewegungsdaten benötigt – stellt sich die Frage, wann die Grundsätze der Arbeitnehmerhaftung überhaupt die Inanspruchnahme zulassen (in der Praxis wird dies nur bei Fällen nachweisbar vorsätzlichen Handelns erfolgsversprechend

sein). So bleibt nur das Interesse des Arbeitgebers, in einem Streit mit Dritten den betreffenden Ex-Mitarbeiter als Zeugen benennen zu können, der dann als „Bürgerpflicht" auch aussagen muss. Aber auch Ansprüche Dritter unterliegen der Verjährung und, wie gesagt, ob die Verjährungsfrist ein zwingendes Argument zur Rechtfertigung des Arbeitgeberinteresses sein kann, ist schon fraglich (s. dazu oben Fall 14).

Man kann aber gerade umgekehrt sogar sagen, dass dem Arbeitgeber eigentlich daran gelegen sein könnte, (überflüssige) Daten des Mitarbeiters möglichst frühzeitig zu löschen, um nicht „uferlose" Auskünfte erteilen zu müssen (s. dazu oben Fall 4). Zudem kann der Mitarbeiter bei einer Interessenabwägung als Legitimationsgrund – wie oben im Fall 22 – der weiteren Verarbeitung widersprechen (Art. 21 DSGVO) und Löschung verlangen, was zumindest zunächst die Einschränkung der Verarbeitung zur Folge hätte (Art. 18 Abs. 1 (d) DSGVO). Dabei ist der Löschzeitpunkt nicht nur für den Verantwortlichen selbst von Belang, sondern muss – wie oben in Fall 22 – eine Mitteilung an andere Verantwortliche, mit denen (bzw. mit deren Mitarbeitern) der Betroffene kommuniziert hat, auslösen. Auch hier zeigt sich, dass eine Trennung der Löschzeitpunkte von unternehmensbezogenen Kontaktdaten und Bewegungsdaten nicht sinnvoll ist, denn ansonsten müssten zwei Mitteilungen versendet werden, je nach Datenkategorie. Und eine selektive Löschung ist weder beim Verantwortlichen noch beim Empfänger der Daten sinnvoll.

- Der Beschäftigte des Kunden / Lieferanten / Dienstleisters

Schließlich ist bei aller Fokussierung auf Bewegungsdaten der Beschäftigten zu bedenken, dass in vielen Fällen eine relevante, wenn nicht überwiegende Menge der vom Beschäftigten erzeugten Kommunikation mit externen Dritten stattfindet. Der oder die externen Kommunikationspartner sind dann ebenso „Betroffene". Dann ist auch dessen bzw. deren mutmaßliche (Interessenabwägung) oder tatsächliche (in der Praxis selten) Einwilligung in eine längere Speicherung (als datenschutzrechtlich für die ursprünglichen Kommunikationszwecke erforderlich) zu prüfen. Zumindest müsste dem dritten Betroffenen die Speicherzeit im Rahmen von Pflichthinweisen kommuniziert werden – und wer tut das schon bei einem gewöhnlichen B2B-Mailverkehr? Die Angabe einer längeren Speicherzeit als nach dem Zweck der Kommunikation oder nach gesetzlichen Aufbewahrungspflichten des empfangenden Verantwortlichen erforderlich – man stelle sich die Angabe „Ihre E-Mail wird bei uns 15 Jahre lang archiviert" in Pflichtinformationen für externe E-Mail-Kommunikationspartner vor – würde bei Adressaten oder bei den Aufsichtsbehörden vielleicht „schlafende Hunde wecken". Insbesondere dann, wenn keine gesetzliche Aufbewahrungspflicht für die konkrete Kommunikation einschlägig wäre, würde damit – aus der Perspektive Dritter – wohl (weit) über das Ziel hinausgeschossen. Solange derartige Kommunikation zwischen Unternehmen

(durch deren Exponenten) personenbezogen im Sinne des Datenschutzrechts ist (s. oben Fall 20), stellen sich solche Fragen.

Diese Fragen spielen bislang in kaum einem Unternehmen eine Rolle. Die meisten Unternehmen gehen vielmehr (unreflektiert) davon aus, dass ihnen die Bewegungsdaten ihrer Mitarbeiter und die B2B-Kommunikationsdaten mit Angehörigen anderer Unternehmen – auch, soweit sie jeweils unternehmensbezogene Kontaktdaten enthalten – „gehören" und sie diese auch nie (!) löschen müssen. Vielleicht haben sie damit sogar Recht, wenn sich ein schlauer Jurist findet, der das begründen kann; und genügend schlaue Juristen können bekanntlich alles begründen. In jedem Fall muss auch hier muss das Vakuum eines „gedankenlosen" Gesetzgebers irgendwie – und mit erheblichen Restrisiken andersdenkender Gerichte und Aufsichtsbehörden – gefüllt werden.

Fall 34:
Daten als Crash Test Dummies?

Praktischer Fall: Die Huber AG entwickelt seit Jahren eine Software für eine digitale Patientenakte. Es steht ein wesentliches neues Release an mit erheblichen Funktionserweiterungen, die vorab geprüft werden müssen. Insbesondere die Skalierbarkeit, d. h. die Verarbeitung der Daten einer großen Anzahl von Patienten, stellt technisch noch ein Problem dar. Die Huber AG ist daher auf der Suche nach möglichst großen Datensätzen mit Beispieldaten, die testweise verwendet werden können, um das System auf Fehlerfreiheit und Performanz zu testen. Der Träger des Krankenhauses in Maieringen, als Anwender auf das System der Huber AG zwingend angewiesen, fragt sich, ob und unter welchen Voraussetzungen bzw. Auflagen er die von ihm verarbeiteten Datensätze der Huber AG zur Verfügung stellen kann.

Software kann nicht hinreichend ohne Daten getestet werden. Der Einsatz von Echtdaten, die aus der produktiven Arbeit mit der Software stammen, für Testzwecke ist daher naheliegend. Eine Anonymisierung dieser Daten ist bisweilen – je nach Datenfeldern und Testzwecken – schwierig bis unmöglich. Teilweise werden Vorabtests in regulierten Bereichen sogar gefordert, ohne dass man hieraus allerdings eine gesetzliche Verpflichtung zum Einsatz von Echtdaten in Testsystemen ableiten kann.

Eine (formularmäßige) Einwilligung der Betroffenen einzuholen würde wohl Probleme mit dem „Koppelungsverbot“ bzw. dem „Entbündelungsgebot“ heraufbeschwören (s. o. Fall 30). Würde das Testsystem, für das die Daten zum Einsatz kommen, unsicherer sein als eine Produktivumgebung, müsste auch darüber wohl informiert werden. Zudem ist eine Einwilligung mit dem Risiko des jederzeit möglichen Widerrufs versehen. Allerdings muss der Widerruf nicht in jedem Fall – außerhalb des Bereichs der Aufbewahrungspflichten – zur sofortigen Löschung führen, sondern die Notwendigkeit der Löschung von noch anderweitig genutzten Daten kann gleichwohl (im Einzelfall) auch einer Abwägung zugänglich sein. So hat es zumindest – ohne dogmatische Begründung, denn in der DSGVO ist dies nicht angelegt – das bayerische Landesamt für Datenschutzaufsicht in seinem Tätigkeitsbericht 2017/2018 im Hinblick auf Mitarbeiterfotos ausgeführt:

„Der Widerruf einer Einwilligung entfaltet Wirkung für die Zukunft (ex nunc). Bei der Frage der weiteren Verwendung der Fotos des betroffenen Mitarbeiters wird eine Abwägung der Interessen der Beteiligten vorzunehmen sein. Dabei ist zugunsten des Unternehmens der

Aufwand bei der Herstellung der Broschüren und Flyer zu berücksichtigen. Die weitere Verwendung der bereits gedruckten Exemplare haben wir als vertretbar angesehen, da die Herstellungskosten sehr hoch waren und der Mitarbeiter keine besonders herausgehobene Funktion im Unternehmen bekleidete und die Darstellung in den Veröffentlichungen ebenfalls nicht besonders herausgehoben war. Bei einer Neuproduktion dürfen die Fotos des betreffenden Mitarbeiters aber nicht mehr verwendet werden.“

Eine solche Interessenabwägung wird sich gleichwohl im Bereich der Testdaten immer dem Einwand ausgesetzt sehen, dass die Verarbeitung der Echtdaten nicht „erforderlich“ ist, sondern auch anonymisierte oder synthetische Daten eingesetzt werden können. Manuell können natürlich immer Echtdaten auch mit Blick auf den Testzweck und die benötigten Datenfelder ausreichend anonymisiert bzw. synthetische (nicht-personenbezogene) Daten hergestellt werden. Dies mag zwar mit erheblichem Aufwand verbunden sein, doch dies allein ist kein taugliches Argument im Rahmen der Bewertung der Erforderlichkeit der Nutzung personenbezogener Daten. Außerdem ist auch die Anonymisierung als solche eine Verarbeitungshandlung, für die es – so behaupten manche Juristen – eine eigene datenschutzrechtliche Legitimationsgrundlage geben muss. Echtdaten dürfen also überhaupt nur zu anonymisierten Testdaten „umgeformt“ werden, wenn es hierfür z. B. eine Einwilligung gibt, deren Widerruf dann allerdings die Anonymisierung (und die weitere Verwendung der gewonnenen anonymen Daten) unberührt blieben ließe. Ähnliche Überlegungen dürften auch im Kontext einer Zweckänderung und des entsprechenden Kompatibilitätstests anzustellen sein.

Diese Themen werden weiter verkompliziert, wenn der Software-Hersteller die Daten nicht selbst „besitzt“, sondern sich von seinen Kunden beschaffen muss. Dann geht es nicht nur um eine mögliche Zweckänderung und ggf. Interessenabwägung, sondern darüber hinaus auch um die Frage, ob eine Übermittlung an Dritte gerechtfertigt werden kann. Dies dürfte noch schwerer zu rechtfertigen sein, was die Frage aufwirft, ob nicht der Software-Hersteller insoweit als Auftragsverarbeiter seines Kunden tätig werden kann. Da allerdings die Ergebnisse der Tests mit den zugelieferten Echtdaten nicht nur dem spezifischen Kunden zugutekommen, kann dies kaum als „Verarbeitung im Auftrag“ dieses spezifischen Kunden gelten.

Fall 35:
Smartphone weg! Was nun?

Praktischer Fall: Die Huber AG hat Frau Maier ein Smartphone zur betrieblichen (E-Mails, Kontakte, Telefonie, Internet etc.) und privaten Nutzung zur Verfügung gestellt. Frau Maier nutzt dieses Smartphone nur sporadisch, findet es aber nun schon seit einer Woche nicht mehr, und gibt nun eine „Vermisstenanzeige" bei der Huber AG auf. Der Datenschutzbeauftragte der Huber AG sinniert, ob er den Vorfall melden soll.

Nach der DSGVO ist eine „Datenpanne" – also auch das „Vermissen" personenbezogener Daten ohne Kenntnis ihres Aufenthaltsorts – binnen 72 Stunden an die zuständige Datenschutzaufsichtsbehörde zu melden. Im gesetzestechnischen Sinne ist eine „Datenpanne" die Verletzung des Schutzes personenbezogener Daten – also nach der Definition in Art. 4 Nr. 12 DSGVO, dass eine *„Verletzung der Sicherheit"* der Daten (im Sinne von Art. 32 DSGVO) vorliegt. Diese Verletzung der Sicherheit muss dazu geführt haben, dass die Daten außerhalb der rechtmäßigen Verarbeitung vernichtet, verloren oder verändert wurden oder dass auch nur eine unbefugte Offenlegung bzw. ein unbefugter Zugang zu den Daten stattgefunden hat (s. dazu auch noch unten Fall 41).

➢ Wie schlimm ist's?

Ist diese Voraussetzung eines Datenschutzverstoßes (Sicherheitsverletzung) erfüllt, besteht die Meldepflicht nur dann nicht, wenn *„die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt"* (Art. 33 Abs. 1 DSGVO). Da es eine vollkommen risikolose Verarbeitung nicht geben kann, ist diese Formulierung als „nur zu einem geringen Risiko führend" zu verstehen. Es muss also im Rahmen einer Risikoanalyse ein „geringes Risiko" von einem „nicht-geringen Risiko" abgegrenzt werden. Die Frage ist nur, was das bedeutet. Die Datenschutzkonferenz hat im Kontext der in Art. 24, 32 DSGVO geforderten Risikobewertung eine Risikomatrix veröffentlicht, wonach der mögliche Schaden und die Eintrittswahrscheinlichkeit zu ermitteln und zu quantifizieren sind (s. dazu noch unten Fall 37). Ein geringes Risiko liegt vor, wenn sowohl der mögliche Schaden als auch dessen Eintrittswahrscheinlichkeit als „gering bis überschaubar" eingeschätzt werden. Nach Empfehlungen aus der Beratungspraxis sollte diese Risikobewertung, bezogen auf die konkrete Datenpanne, *„bestenfalls von einem außenstehenden unabhängigen Gutachter vorgenommen werden, damit sich das Unterneh-*

men im Falle einer möglichen Datenschutzverletzung auch gegenüber einer Aufsichtsbehörde entsprechend positionieren kann". Da sollte das eine oder andere Unternehmen wohl am besten gleich einmal feste Kontingente bei „unabhängigen Gutachtern" buchen.

➢ Wie wahrscheinlich ist die Überwindung der Sicherheitshürden?

Im Vorfeld der Risikobewertung ist das verantwortliche Unternehmen (natürlich) zu einer Aufklärung des entsprechenden Sachverhalts verpflichtet. Der Verantwortliche kann sich nicht darauf berufen, er habe mangels Kenntnis der Details keine Meldung vornehmen können. Aber der Verantwortliche muss auch den zugrundeliegenden technischen Basissachverhalt (Verwendung unternehmenseigener Smartphones) bewertet und (risikoabhängig) „im Griff" haben, und zwar schon vor der konkreten Anwendung (Art. 25 Abs. 1 DSGVO). Bei einem Smartphone stellt sich in diesem Zusammenhang – wie auch bei anderen mobilen IT-Geräten – die Frage, wie sicher die Daten im Hinblick auf einen Zugriff Dritter sind, der das Gerät in die Hand bekommt. Ist der Inhalt des Geräts verschlüsselt? Welche Verschlüsselungsform bzw. welcher Zugangsschutz liegt vor (Datenträgerverschlüsselung, Kennwortschutz)? Wie komplex ist das verwendete Kennwort? Wurde es irgendwo zugänglich aufbewahrt (Sticker am Monitor etc.)? Mit welchen Hilfsmitteln kann der Inhalt auch ohne Kenntnis des Kennworts entschlüsselt werden („brute force"-Angriff, Software- oder Hardware-Lücke)? Vielleicht gibt es Methoden, den Schutz zu „knacken", die in der Öffentlichkeit noch gar nicht bekannt sind? Hat sich insoweit etwas Neues ergeben (s. zur „Monitoring-Pflicht" oben Fall 32)? „Unknackbare" Geräte gibt es schlichtweg nicht.

Natürlich ist – wie immer – streitig, ob eine Verschlüsselung der Daten dazu führt, dass von keinem relevanten Risiko ausgegangen werden darf. Nach dem Datenschutz- und Informationsfreiheitsbericht 2019 der Landesdatenschutzbeauftragten in Nordrhein-Westfalen ist ein Schadenseintritt höchst unwahrscheinlich, wenn die Daten „sicher verschlüsselt" sind – was immer das heißt. Der Vorfall ist dann nicht an die Behörde zu melden, sondern „nur" intern zu dokumentieren und die entsprechenden Maßnahmen zu ergreifen, um künftig solche Vorfälle zu vermeiden. Wie soll das beim Verlust eines Smartphones umgesetzt werden? Anketten?

➢ Auch das noch!

Im Übrigen hätte Frau Maier, die das Smartphone auch privat nutzt und damit entsprechend Verantwortliche für die privat genutzten Daten (Kontaktdaten, Chats etc.) ist, diese Risikoabwägung auch selbst anstellen müssen (s. oben Fall 18). Dann ist es natürlich zumindest „er-

klärungsbedürftig“, wenn einer der Verantwortlichen – der Arbeitgeber oder der Arbeitnehmer als Privatperson und Verantwortlicher der privaten Daten – eine solche Meldung abgibt, der andere aber nicht.

- Benachrichtigung der Betroffenen?

Ein deutsches Elektronikversandunternehmen veröffentlichte im November 2019 auf seiner Website die Information, dass Unbekannte über Monate hinweg auf 14 Millionen (unverschlüsselte) Kundendatensätze zugreifen könnten. Die Daten umfassten Postadressen, teilweise E-Mail-Adressen, Fax- und Telefonnummern sowie bei ca. 2,8 Millionen Datensätzen auch IBAN-Daten der Kunden. Bei der Aufklärung arbeitete das Unternehmen nach eigenen Angaben eng mit dem zuständigen Bayerischen Landesamt für Datenschutzaufsicht zusammen. Die Kunden wurden nicht, wie von Art. 34 DSGVO Abs. 1 DSGVO vorgegeben, individuell benachrichtigt (die Information auf der Webseite stellt keine individuelle Benachrichtigung dar).

Dies wirft die Frage auf, wann im Rahmen einer Datenpanne ein „hohes Risiko“ für die Betroffenen vorliegt, sodass diese nach Art. 34 DSGVO zu informieren sind. Die Abwägung der Risiken für die „Rechte und Freiheiten natürlicher Personen“ wird noch unten in Fall 37 im Detail dargestellt. In Bezug auf die Kundeninformationen im oben geschilderten Fall kann hier zunächst festgehalten werden, dass mit den IBAN-Informationen spezifische Zahlungsinformationen „entkommen“ konnten (Risiko des Missbrauchs des Lastschriftverfahrens). Die E-Mail-Adressen können – ggf. unter Zuhilfenahme von Namen, Adressen und Telefonnummern, was den Anschein der Rechtsmäßigkeit erhöht – für Malware oder Phishing-Mails missbraucht werden. Mittels der Telefonnummern (aber auch der Adressen, dort nur mit höherem Aufwand) können die Kunden belästigt werden. Ob dies nun ein „hohes Risiko“ für die Betroffenen bedeutet, mag jeder selbst entscheiden.

Im Ausgangsfall wäre eine genügend „starke“ Verschlüsselung hingegen schon geeignet, auch bei sensiblen Daten – und damit „eigentlich“ hohem Risiko – die Information an die Betroffenen jedenfalls entfallen zu lassen. Dies wurde ausnahmsweise relativ ausdrücklich geregelt (Art. 34 Abs. 3 lit. a DSGVO).

Fall 36:
Unter der Haube, in den Wolken

Praktischer Fall: Die Huber AG verwendet seit langer Zeit auf ihren Büro-PCs und ihren Servern das Betriebssystem Windows und das Bürosoftware-Paket „Office" von Microsoft. Frau Müller – die den Unternehmens-PC auch für gelegentliche private Zwecke nutzen darf – ist in der Buchhaltung der Huber AG tätig und fragt sich, welche Daten über sie auf diese Weise an Microsoft abgeflossen sind und ob nicht auch die Huber AG ihr gegenüber diesbezüglich rechenschaftspflichtig ist.

Jedes Unternehmen setzt ja heutzutage allerhand IT ein. Manchmal weiß ein Unternehmen gar nicht, wie viel und welche IT überall eingesetzt wird. Kaum ein Unternehmen kommt an Windows vorbei, und die meisten der Unternehmen, die Windows als Betriebssystem nutzen, nutzen auch Office. Dabei ist wichtig darauf hinzuweisen, dass sicherlich auch andere Betriebssysteme und Anwendungen über die nachfolgend behandelten ständigen Online-Verbindungen zu ihren Herstellern verfügen, aber vielleicht noch nicht so gut „erforscht" sind wie die Sammlung von (u. a.) Telemetrie-Daten durch diese Microsoft-Produkte. Dies betrifft Betriebssysteme für Mobiltelefone oder Tablets (Android, iOS) wie auch Anwendungen und Apps, die Daten an die Betreiber- bzw. Hersteller-Server übertragen. Selbst wenn Microsoft unter dem öffentlichen Druck die Erhebung und Übermittlung von Daten an die US-Zentrale immer weiter transparent gemacht und zwischenzeitlich auch stärker konfigurierbar ausgestaltet hat, bleibt das grundsätzliche Problem im Verhältnis zwischen Software-Hersteller (oder Dienst-Betreiber) einerseits und dem Anwender (bzw. Unternehmenskunden) andererseits bestehen. Es geht daher hier eigentlich nicht spezifisch um „den Microsoft-Fall", sondern dieser steht als Beispiel für ein grundsätzliches Problem in der (Unternehmens-) Praxis.

➢ Übermittlung durch die Hintertür

Sowohl niederländische als auch deutsche Behörden haben verschiedene Untersuchungen bzw. Datenschutz-Folgenabschätzungen zu Microsoft-Produkten in Auftrag gegeben. Es ging jeweils im Prinzip darum, ob und welche personenbezogenen Daten die Software an Microsoft-Server übermittelt, wenn sie „nach Hause telefoniert". Für die Kontaktaufnahme mit den Microsoft-Servern in den USA gibt es verschiedene Gründe, darunter natürlich der Bezug automatischer Updates und die Überprüfung einer gültigen Lizenz. Ein anderer Grund ist die Übermittlung von sogenannten „Telemetrie-Daten". In der Technik wird damit üblicherweise die automatisierte, laufende Übertragung von Sensordaten beweglicher technischer

Objekte wie Fahr- oder Flugzeuge an eine „Zentrale“ bezeichnet, in der die Daten – insbesondere zu Zwecken der Verbesserung der technischen Eigenschaften – analysiert werden.

Eine Software wie Windows oder Office, die millionenfach „im Feld“ eingesetzt wird, kann bei ständiger Internet-Anbindung zur Analyse des Nutzerverhaltens und damit auch für die Untersuchung von Fehlern (bis hin zu Abstürzen – sog. „*crash dump*“) verwendet werden. Mit den an die verschiedenen Microsoft-Server im Laufe der Zeit übertragenen Daten kann aber auch ein Profil des identifizierbaren Nutzers gebildet werden.

Nach einer Rahmen-Datenschutz-Folgenabschätzung für das Niederländische Ministerium für Justiz und Sicherheit vom Juni 2019 sammelt Windows 10 etwa 1200 verschiedene Ereignis-Typen. Diese Ereignisse werden bei Microsoft (in den USA) analysiert. Microsoft kann neue Ereignis-Typen zu den Telemetrie-Daten hinzufügen, ohne dass dies den Nutzern auffällt. Die Telemetrie-Daten enthalten verschiedene geräte- und nutzerspezifische IDs, die Microsoft den Aufbau eines Nutzerprofils erlauben und letztlich auch – etwa über Domain-Namen – Personen zugeordnet werden können. In der Datenschutz-Folgenabschätzung vom Juni 2019 werden die – durch den „Diagnostic Data Viewer“ vom Benutzer zwischenzeitlich selbst einsehbaren – Daten wie folgt zusammengefasst:

„A typical telemetry event contains a unique number, a timestamp, several unique identifiers for the end-user and the device, and different bits of information about for example the hardware that is used, the screen size, operating system, applications installed and usage details, as well as reliability information on device drivers.“

Die Übertragung von Telemetrie-Daten kann Windows-intern zwar beschränkt werden, aber die größte Minimierung kann – neben der Blockade des entsprechenden Netzwerkverkehrs durch den Administrator mit speziellen (Drittanbieter-) Werkzeugen – nur mit der „Enterprise“-Version von Windows erreicht werden. Selbst mit der rigidesten Windows-Einstellung werden immer noch – wenn auch erheblich weniger – personenbezogene Daten erhoben. Die Daten werden nach den Erkenntnissen der niederländischen Datenschutzaufsichtsbehörde teils 30 Tage, teils 13 Monate, teils 37 Monate lang gespeichert – Microsoft selbst macht hierzu keine öffentlichen Angaben. Der Abfluss von Inhaltsdaten (Datei- oder E-Mail-Inhalte) konnte bei der Analyse „nicht beobachtet“ werden; grundsätzlich wäre aber auch denkbar, dass ein Hersteller derartige Daten in verschlüsselter Form und in kleinen „Häppchen“ zu sich überträgt. Dass (zumindest) Teile des Datenverkehrs verschlüsselt werden, war im Rahmen der Untersuchungen offensichtlich. So funktionierten etwa Microsoft-Apps nicht mehr, wenn im Rahmen der Analysen der Netzwerkverkehr in spezifischer Weise überwacht

wurde – die Apps bauen einen sicheren (verschlüsselten) „Tunnel“ für den Datenverkehr von und zu Microsoft auf, was unter den Bedingungen der Überwachung nicht mehr möglich war. Im Grundsatz wurden diese Erkenntnisse – und dass eine vollständige „Entkoppelung“ von Microsoft zwar (technisch durch Drittprodukte) möglich, aber für den Anwender schwer umzusetzen ist – auch vom (deutschen) BSI im Rahmen von dessen Projekt „SiSyPHuS Win10“ bestätigt. Dieses Projekt bezieht sich allerdings noch auf die Version 1607 von Windows 10.

Die für die Telemetrie-Daten einschlägigen Datenschutzbestimmungen von Microsoft enthielten mehrere und sehr weit gefasste Zwecke, welche die Verwendung der Daten etwa auch für Werbung erlauben. Zwischenzeitlich hat die niederländische Regierung allerdings für sich (!) die Beschränkung der Zwecke für sämtliche von Microsoft im Rahmen von Online-Services bzw. für Office 365 ProPlus erhobenen Daten auf drei herunterverhandelt (Bereitstellung und technische Verbesserung des Dienstes, Aktualisierung des Dienstes und Sicherheit) und entsprechende Audit-Rechte vereinbart. Inwieweit das auch für Windows 10 gilt, ergibt sich aus den maßgeblichen Presseerklärungen nicht. Außerdem hat Microsoft die Geschäftsbedingungen für Cloud-Dienste bei kommerziellen Kunden dahingehend überarbeitet, dass Microsoft in verschiedenen Konstellationen ausdrücklich seine Rolle als Verantwortlicher bestätigt (wobei die datenschutzrechtlichen Rollen ohnehin nicht vertraglich „festgelegt“, sondern nur konkretisiert werden können (s. dazu oben Fall 16). Die DSGVO-Risiken für Microsoft-Produktnutzer haben also – wenn auch eher für Unternehmen, die insbesondere Beschäftigtendaten verarbeiten, als für private Anwender, die natürlich auch Verantwortliche im Sinne der DSGVO sein können (s. oben Fall 18) – bereits stufenweise abgenommen, je mehr Microsoft auf den Druck (insbesondere der öffentlichen Hand) reagiert.

Eine Übermittlung der personenbezogenen Daten in die USA (Drittlandsübermittlungsgrundlage) kann zwar sowohl mit dem US-EU-Privacy-Shield als auch mit der Verwendung der Standardvertragsklauseln der EU-Kommission rechtfertigt werden, doch sind beide Mechanismen derzeit „unter Beschuss“. Eine Liste der eingesetzten Auftragnehmer (Auftragsverarbeiter) liegt nicht vor. Daneben bestehen auch Zweifel, welche Legitimationsgrundlage für die Übermittlung an sich einschlägig ist bzw. rechtfertigt werden kann.

Die Informationspolitik der Software-Hersteller dazu ist häufig „schmallippig“, wie sich auch aus der Datenschutz-Folgenabschätzung im Hinblick auf Microsoft ergibt:

„Microsoft does not provide a public explanation why it is necessary to transmit all telemetry data to servers in the USA, why not store these in the EU, or at least, anonymise the data collected in the EU before they are transferred to the USA."

Ein besonderes Risiko für den Unternehmenskunden – hier die Huber AG – ist, dass der Software-Hersteller bzw. Dienst-Betreiber (Microsoft) und der Unternehmenskunde gegenüber den Beschäftigten des Unternehmenskunden im Hinblick auf die erhobenen und übermittelten Telemetrie-Daten eine Stellung als gemeinsam Verantwortliche haben. Der Unternehmenskunde ermöglicht es dem Software-Hersteller bzw. Dienst-Betreiber, die Daten „abzusaugen" und zu analysieren (s. dazu oben Fall 16). Wird dann die von Art. 26 DSGVO geforderte Vereinbarung nicht zur Verfügung gestellt bzw. abgeschlossen, ergeben sich schon deswegen – ähnlich wie für Facebook-Fanpage-Betreiber – erhebliche Risiken. Dieses Risiko ist vielen Verantwortlichen nicht bewusst, weil sie – im Ansatz richtigerweise – davon ausgehen, dass sie ihre Software *„on premise"*, d. h. auf ihren eigenen IT-Anlagen, betreiben und selbst darüber entscheiden können, welche (Beschäftigten-) Daten das Unternehmen verlassen.

Daneben gibt es natürlich auch Software, die komplett „in der Cloud" ausgeführt wird, also auf Servern, die außerhalb des Verantwortlichen betrieben werden und über die der Verantwortliche – im Gegensatz zu einer selbst mit aufgebauten Infrastruktur in einem beauftragten Rechenzentrum – „nicht viel weiß". Hierzu zählt das oben schon erwähnte Office-Paket „Office 365" von Microsoft. Neben der fest installierten Office-Variante gibt es hier zusätzlich mobile Apps für Android und iOS sowie einen Software-as-a-Service-Dienst, der im Browser lauffähig ist (ähnlich einem Remote-Desktop, d. h. Tastatur- und Maus-Daten werden übertragen und die „Reaktion" wird als Bildschirminhalt übermittelt). Hierbei werden neben Inhalts- und Diagnosedaten auch „Funktionsdaten" übermittelt, mit denen die auf den Servern ablaufende App „ferngesteuert" wird. Daneben fallen im Rahmen der sog. „Connected Experiences" wie Rechtschreibprüfung, Übersetzung und Office-Hilfe Daten an.

➢ Rechtliche Einordnung

Der Verantwortliche im datenschutzrechtlichen Sinne, sprich der Benutzer solcher Services (hier die Huber AG), muss sich im Vorfeld des Einsatzes von Software auf mit dem Internet verbundenen IT-Systemen wie auch bei der Auslagerung von Funktionalitäten „in die Cloud" Gedanken zur datenschutzrechtlichen Einordnung und Zulässigkeit machen. Auch hier gilt: Soweit der Dritte (hier Microsoft) ein eigenständiger Verantwortlicher ist, muss sich die Huber AG überlegen, wie sie den Empfänger ggf. vertraglich binden muss, um die fortwirkende Zweckbindung sicherzustellen (s. oben Fall 12). Soweit der Dritte ein Auftragsverarbeiter ist

(s. oben Fall 7), muss die Huber AG die Vorgaben des Art. 28 DSGVO einhalten. Beispielsweise muss die Huber AG sicherstellen, dass der Dritte „Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermögliche und dazu beiträgt“ (Art. 28 Abs. 3 lit. h DSGVO). Soweit der Verantwortliche und der Dritte die Stellung von gemeinsam Verantwortlichen (s. oben Fall 16) haben, müssen beide sicherstellen, dass sie die Vorgaben des Art. 26 DSGVO erfüllen und daneben für die Verarbeitungsphasen, für die sie gemeinsam verantwortlich sind, die DSGVO-Konformität der Verarbeitung sicherstellen.

Dabei kann es durchaus sein, dass der Verantwortliche und der Dritte unterschiedliche Auffassungen darüber haben, welche der oben genannten Konstellationen vorliegt, welche vertraglichen Abreden notwendig sind und inwieweit sich der Dritte „in die Karten schauen“ lassen muss. Bei einem Verantwortlichen mit Sitz in einem Drittland können unterschiedliche Auffassungen über die Drittlandsübermittlungsgrundlage bestehen.

- Der Verantwortliche als Detektiv

Und schließlich stellt sich auch die Frage, inwieweit die Tätigkeit des Dritten vom Verantwortlichen überhaupt aktiv erforscht wird, d. h. ob diese mit seinen (vertraglichen) Aussagen in Einklang steht. Der Umfang und die Beschaffenheit der Telemetrie-Datenströme hat Microsoft nicht selbst offengelegt, sondern dies bedurfte einer (kosten-) intensiven „Detektivarbeit“. Es ist nicht bekannt, dass Unternehmen der Privatwirtschaft für den Einsatz derartiger Produkte solche Datenschutz-Folgenabschätzungen mit granularen IT-Untersuchungen durchgeführt haben wie dies etwa die niederländischen Behörden beauftragt haben. Vielleicht ist diese Information aber auch nur nicht nach draußen gedrungen. Zumindest dürfen Unternehmen, die bislang auf vertragliche Aussagen vertraut oder mögliche Szenarien nicht selbstständig erkannt oder weiter durchdacht haben, nach öffentlicher Information über derartige Datenabflüsse nicht „nichts tun“, sondern dies in ihre – ständig zu aktualisierende – Risikobewertung einfließen lassen.

Nicht umsonst haben Umfang und Komplexität der Microsoft-Datenverarbeitung u. a. dazu geführt, dass die Bremer Datenschutzaufsichtsbehörde mit einem umfangreichen Fragebogen Unternehmen zur Nutzung von Office 365 befragt hat. Eine der Fragen lautet (natürlich), ob im Vorfeld der Nutzung eine Datenschutz-Folgenabschätzung (s. dazu oben Fall 35) durchgeführt wurde und wenn nein, warum nicht. Das Thema Risikobewertung der Verarbeitungsprozesse des Verantwortlichen ist zufälligerweise auch gleich das Thema des nächsten Falles 37. Nach einem Urteil des Verwaltungsgerichts Mainz vom Mai 2019 darf eine

Datenschutz-Aufsichtsbehörde Auskunft in Form von Fragenkatalogen auch als Verwaltungsakt gegenüber dem Verantwortlichen begehren und die Beantwortung mit Verwaltungszwangsmaßnahmen durchsetzen.

- Härtungsempfehlungen

Das vom Niederländischen Ministerium für Justiz und Sicherheit eingeschaltete IT-Beratungsunternehmen kommt immerhin zu folgenden „Tipps“ an die IT-Administratoren – auch als „Härtungsempfehlungen“ bezeichnet –, in deren Unternehmen die genannten Produkte eingesetzt werden, und schätzt das dann verbleibende Verarbeitungsrisiko nicht mehr als „hoch“ ein:

„Aktualisieren Sie auf Version 1905 oder höher von Office 365 ProPlus und stellen Sie die Telemetrie auf das Niveau "Neither" ein. Nutzen Sie die technische Möglichkeit, die Nutzung der Controller Connected Experiences in Office 365 ProPlus zu verbieten (zusätzliche Connected Experiences deaktivieren). Deaktivieren Sie das Customer Experience Improvement Program (CEIP) in Office ProPlus. Deaktivieren Sie die LinkedIn-Integration für Microsoft-Mitarbeiterkonten in Office ProPlus. Richten Sie Richtlinien ein, um die Mitarbeiter vor der Verwendung der mobilen Office-Apps und der Controller Connected Experiences in Office Online zu warnen, bis die fünf hohen Risiken gemildert sind. Wählen Sie so schnell wie möglich die niedrigste und minimalste Stufe der Erfassung von diagnostischen Daten in Office Online und den mobilen Apps. Aktualisieren Sie Ihre interne Datenschutzrichtlinie für den Umgang mit personenbezogenen Daten der Mitarbeiter mit spezifischen Informationen für welche Zwecke und unter welchen Umständen das Unternehmen verschiedene Arten von diagnostischen Daten aus den verschiedenen Diensten und Produkten von Microsoft anschauen kann. Führen Sie Datenschutz-Folgenabschätzungen durch, bevor Sie Workplace Analytics und Activity Reports im Microsoft 365 Admin Center verwenden und bevor Mitarbeiter MyAnalytics und Delve nutzen können. Erwägen Sie die Verwendung von Customer Lockbox und Customer Key, abhängig von der Empfindlichkeit der Inhaltsdaten. Aktualisieren Sie auf die Version 1903 von Windows 10 Enterprise, um Intune mit Security-Telemetrie zu verwenden. Stellen Sie das Telemetrie-Niveau in Windows 10 Enterprise auf Security oder blockieren Sie den Telemetrieverkehr und erlauben Sie es Benutzern nicht, ihre Aktivitäten über die Timeline-Funktionalität zu synchronisieren. Berücksichtigen Sie mögliche Änderungen für die Validität von Datentransfermechanismen (wie das EU-US Privacy Shield) aufgrund der künftigen Rechtsprechung des Europäischen Gerichtshofs. Es liegt an dem Europäischen Gerichtshof, die Risiken der massenhaften Überwachung in den Vereinigten Staaten zu bewerten, und an dem europäischen Gesetzgeber, die verbleibenden Risiken der Übermittlung von diagnostischen Daten aus der EU in die USA zu verringern.“

Angesichts all dieser Umstände kann es nicht verwundern, dass die Datenschutzkonferenz im November 2019 ein „Prüfschema“ unter der Bezeichnung „Datenschutz bei Windows 10“ herausgegeben hat. Hiernach sollen Verantwortliche zunächst bestimmen, welche Daten sie mit welcher Version / Edition von Windows 10 verarbeiten wollen. Die auf dieser Basis

„festgestellten Datenübermittlungen und die damit verbundenen Übermittlungen von personenbezogenen Daten sind auf ihre Rechtmäßigkeit zu prüfen. Die möglichen Rechtsgrundlagen hängen von der jeweiligen Funktion und den übermittelten Daten ab. Soweit für die Übermittlung eine Rechtsgrundlage vorliegt, kann Windows 10 oder können bestimmte Funktionen von Windows 10 genutzt werden. Konnte nicht festgestellt werden, welche Daten übermittelt werden, so kann auch nicht die Rechtmäßigkeit der Übermittlung festgestellt werden.“

Schon dies dürften die wenigsten Unternehmen „wirklich“ leisten können. Es schließt sich dann die Definition und Implementierung angemessener technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO an, die auch im Blockieren von Netzwerkverkehr bestehen können. Diese Maßnahmen sind nach jedem Update neu zu evaluieren. Daneben ist eine Bewertung des trotz der getroffenen Maßnahmen verbleibenden Restrisikos durchzuführen. Das Restrisiko muss „tragbar“ sein – was das bedeutet, ist allerdings unklar (s. dazu auch unten Fall 37). Die Handlungsvorschläge enden mit dem schönen Satz *„Wenn das Restrisiko durch die Implementierung der Maßnahmen tragbar ist, kann Windows 10, bzw. können bestimmte Funktionen von Windows 10 zum Einsatz kommen.“* Was das alles konkret bedeutet und welcher Aufwand vom Unternehmen zu betreiben ist, bleibt, wie so häufig, im Dunkeln.

Fall 37:
Die Risikofrage – Wie viel setzen Sie?

Praktischer Fall: Die Huber AG verarbeitet verschiedene personenbezogene Daten, nämlich

- *Personalaktendaten ihrer Beschäftigten,*
- *Notfallkontakte ihrer Beschäftigten (zumeist Verwandte wie Ehegatten oder Kinder),*
- *Bewegungsdaten ihrer Beschäftigten (wie Änderungsbelege in der ERP-Software, welche sowohl den handelnden Mitarbeiter als auch den ursprünglichen und den neuen Feldinhalt ausweisen),*
- *Ansprechpartner von Unternehmen, welche die Huber AG mit Waren und Dienstleistungen beliefern (B2B-Lieferanten) oder von der Huber AG Waren und Dienstleistungen beziehen (B2B-Kunden), wobei es sich dabei auch um Einzelkaufleute, Freiberufler oder Ein-Mann-GmbHs handeln kann,*
- *Kontaktdaten von Kontaktpersonen in Verbänden und politischen Parteien sowie allgemein zu Marketing-Zwecken, mit denen die Huber AG irgendwann in Kontakt stand bzw. steht und die sich in Zukunft noch als nützlich erweisen könnten.*

Die Huber AG führt eine datenschutzrechtliche Risikobewertung durch und fragt sich, welches datenschutzrechtliche Risiko – niedrig, normal, hoch – mit der Verarbeitung dieser Daten einhergeht.

Man muss nicht zu der Generation gehören, die am Samstagabend noch „Der große Preis" mit Wim Thoelke schaute, um zu erahnen, was wohl damals die „Risikofrage, wie viel setzen Sie?" war. Tatsächlich ist die Risikobewertung ein essentieller Bestandteil eines Datenschutz-Compliance-Management-Systems, denn das Datenschutzrecht ist „risikobasiert": Insbesondere hängen die notwendigen technischen und organisatorischen Maßnahmen vom Risikogehalt der jeweiligen Daten bzw. Verarbeitung ab (insbes. Art. 24, 25, 32 DSGVO). Wer allerdings denkt, man könnte Risiko schön sauber auf die Nachkommastelle genau quantifizieren und die daraus folgenden Maßnahmen mit „mathematischer" Präzision bestimmen, wird an den nachfolgenden Ausführungen keine rechte Freude haben.

Vonseiten der Datenschutzbehörden beschäftigen sich sowohl das Kurzpapier Nr. 18 als auch das Standard-Datenschutzmodell mit der Risikobewertung, letzteres sowohl in dessen Abschnitt D3.1 bis D3.4 als auch in dessen Baustein 41 („Planung und Spezifikation"). Nach dem Standard-Datenschutzmodell fließt das ermittelte Risiko *„in dreierlei Form in die weiteren Betrachtungen ein"* (Abschnitt D4.3): Erstens findet das Risiko irgendwie Eingang in die qualitative Konkretisierung der Gewährleistungsziele bezüglich der (konkreten) Verarbeitungstätigkeit. Zweitens wirkt das Risiko irgendwie als Faktor auf die Abwägung zwischen

der Wahrung der Interessen der Betroffenen und dem hierfür erforderlichen Aufwand des Verantwortlichen ein. Drittens fließt das Risiko irgendwie in die Bewertung der nach Umsetzung von technischen und organisatorischen Maßnahmen verbleibenden Restrisiken ein.

Die Aufgabe, eine datenschutzrechtliche Risikobewertung durchzuführen, muss nach der DSGVO jeder Verantwortliche – ob Privatmann oder Großkonzern – gleichermaßen bewältigen. Wer die nachfolgenden Ausführungen liest, die sich mit den verschiedenen Szenarien, Umständen und Folgen beschäftigen, die „gefahrerhöhend" wirken und damit zu einem „hohen Verarbeitungsrisiko" führen können, dem mag einiges unausgegoren und unklar erscheinen. Gerade am Beispiel Risikobewertung, mit einem häufig mutmaßlich als „gegriffen" oder sogar „willkürlich" empfundenen Ergebnis, zeigt sich, wie „unpraktisch" (im Sinne von „schlecht rechtssicher operationalisierbar") die DSGVO ist.

- Risiko von was?

Im Rahmen der Planung eines Datenschutz-Management-Systems ist für jede Datenkategorie zunächst das Risiko für die Rechte und Freiheiten Betroffener durch die Verarbeitung für den Fall zu bestimmen, dass die Daten zum vorgesehenen Zweck verarbeitet werden und noch keine zusätzlichen technischen und organisatorischen Maßnahmen getroffen werden (Baustein M41.08 des Standard-Datenschutzmodells). Aus diesem (abstrakten) Risiko ergibt sich dann der Schutzbedarf der Betroffenen. Es ist umso höher, je sensibler die verarbeiteten Daten sind. Die „Rechte und Freiheiten der betroffenen Personen" beziehen sich – so die Datenschutzbehörden – hauptsächlich auf das „Recht auf Datenschutz" (Art. 8 Abs. 1 der Europäischen Grundrechtecharta) als Ausprägung der informationellen Selbstbestimmung, *„aber auch auf andere Grundrechte wie Rede- und Gedankenfreiheit, Freizügigkeit, Benachteiligungsverbot, Recht auf Freiheit, Gewissens- und Religionsfreiheit"*. Dieses ziemlich „uferlose" Schutzgut wird übrigens unter Datenschutz-Theoretikern unter dem Stichwort „Schutzgutdebatte" diskutiert.

Aufgrund der Qualität dieser (Grund-) Rechte geht es in der Praxis freilich in erster Linie um immaterielle Schäden für die Betroffenen (so das oben angesprochene Kurzpapier Nr. 18). Neben dem Risiko von Schäden aus der geplanten Verarbeitung selbst (zum vorgesehenen Zweck) können sich Schäden aus einer eigenverantworteten oder fremdverursachten Abweichung von der bezweckten Verarbeitung ergeben. Diese Schäden können – ebenso wie im Bereich der Informationssicherheit – die Folge eines Verlusts der Verfügbarkeit der Daten, der Vertraulichkeit von Informationen sowie der Integrität (inhaltlichen Richtigkeit) von Informationen sein.

➢ Datenschutz-Folgenabschätzung und Schwellwertanalyse

Hat in diesem Zusammenhang *„eine Form der Verarbeitung [...] aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“*, ist vorab eine Datenschutz-Folgenabschätzung durchzuführen (Art. 35 DSGVO). Dabei ist allerdings schon unklar, nach welchen Kategorien die DSGVO Risiken überhaupt bemisst: Sie selbst nennt alternativ ein normales und ein hohes Risiko, aber auch ein „Nicht-Risiko“ (Art. 33 DSGVO), das von den Datenschutz-Behörden sinngemäß als „unwesentliches Restrisiko“ umschrieben wird (da es ein Null-Risiko nicht geben kann).

Die Datenschutz-Folgenabschätzung selbst ist ein Verfahren, anhand dessen die Verarbeitung beschrieben, ihre Notwendigkeit und Verhältnismäßigkeit bewertet und die Risiken für die Rechte und Freiheiten natürlicher Personen, die die Verarbeitung personenbezogener Daten mit sich bringt, durch eine entsprechende Risikoabschätzung und die Ermittlung von Gegenmaßnahmen besser kontrolliert werden sollen. Sie unterscheidet sich von der in jedem Fall vorzunehmenden „normalen“ Risiko- und Schutzmaßnahmenbestimmung durch ein höheres Maß an Formalisierung und die ggf. notwendige Einbeziehung Dritter. Was genau das heißt, ist unklar; das Interpretationspapier der Aufsichtsbehörden zur Durchführung einer Datenschutz-Folgenabschätzung (Kurzpapier Nr. 5 der Datenschutzkonferenz) bleibt naturgemäß vage. Jedenfalls handelt es sich nicht um eine einmalige Aufgabe, sondern um einen kontinuierlichen Prozess (Überprüfung und Erneuerung). Hier wird also niemandem die Arbeit ausgehen.

Ob ein hohes Risiko im beschriebenen Sinne vorliegt, ist im Rahmen der sog. Schwellwert-Analyse zu ermitteln. Diese „Vor-Risikoanalyse“ sollte dann gleichzeitig im Kontext der von der DSGVO ohnehin geforderten „gewöhnlichen“ Risikoanalyse Anhaltspunkte für das generelle Risiko geben: Führt die Schwellwert-Analyse zu keinem hohen Risiko, so sollte auch die „gewöhnliche“ Risikoanalyse nicht mehr zu einem hohen Risiko führen.

➢ Der Gesetzestext

Im Einzelnen ist unklar, wie genau eine Schwellwert-Analyse zur Ermittlung eines „hohen“ Risikos durchzuführen ist. Die DSGVO selbst gibt keine klaren – und vor allem abschließenden – Kriterien vor. Dementsprechend ist auch der materielle Maßstab der Schwellwertanalyse in seinen Einzelheiten offen, etwa, ob sich das „hohe Risiko“ kumulativ auf die Art, den Umfangs, die Umstände und den Zwecke der Verarbeitung beziehen muss oder ob einzelne Elemente ausreichen. Erwägungsgrund 76 führt hierzu nur aus:

„Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt."

Eine stringente Methodik für die Bewertung sucht man in der DSGVO vergebens, denn auch in Art. 35 Abs. 1 und 3 DSGVO ist nur von (nicht-abschließenden) „insbesondere"-Fällen die Rede. Dort werden insgesamt vier Konstellationen genannt, nämlich die *„Verwendung neuer Technologien"* in Art. 35 Abs. 1 DSGVO und weitere drei Konstellationen in Art. 35 Abs. 3 DSGVO, von denen Art. 35 Abs. 3 lit. a und b DSGVO nachfolgend wiedergegeben werden. Daneben kann dann noch – wie so oft – im Kaffeesatz der Erwägungsgründe gelesen werden.

Werden sensible Kategorien von personenbezogenen Daten im Sinne von Art. 9 und 10 DSGVO „umfangreich" verarbeitet, so ist eine Datenschutz-Folgenabschätzung durchzuführen (Art. 35 Abs. 3 lit. b DSGVO). Nur: Was heißt eigentlich „umfangreich"? Wenn ein mittelständisches Unternehmen 400 Mitarbeiter beschäftigt und von sämtlichen Mitarbeitern aus Gründen der abzuführenden Kirchensteuer deren Konfession erhebt, verarbeitet es dann „umfangreich" sensible Kategorien personenbezogener Daten? Einen – wenig erquicklichen – Anhaltspunkt liefert Erwägungsgrund 91:

„Dies sollte insbesondere für umfangreiche Verarbeitungsvorgänge gelten, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und [...]. Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein."

Auch das erklärt nicht, wo die Grenze zwischen einem „Ein-Mann-Freiberufler" und einer „großen Menge personenbezogener Daten auf regionaler Ebene" liegt – immerhin befindet sich dazwischen ein weites Feld.

Unabhängig davon: Findet „*eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen*“ statt, „*die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen*“, ist ebenfalls eine Datenschutz-Folgenabschätzung durchzuführen (Art. 35 Abs. 3 lit. a DSGVO). Für derartige „persönliche Aspekte“ enthält Erwägungsgrund 75 einige Beispiele (s. u.). Aber welches CRM-System („automatisierte Verarbeitung“) erlaubt nicht die Eingabe persönlicher „Track Records“ zu jedem Kontakt mit einem möglichen Kunden, anhand derer dann – in systematischer Bewertung persönlicher Aspekte wie persönlicher Vorlieben und Interessen – entschieden wird, ob und wie der Betreffende weiter angesprochen wird?

Neben diesen Fallgruppen, die sich jeweils aus bestimmten Datenkategorien und qualifizierenden Verarbeitungsmerkmalen zusammensetzen („umfangreich“, „systematisch und umfassend“), enthalten die in Erwägungsgrund 75 dargestellten Fälle von „*Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere –*“ sozusagen die „Basiszutaten“ der allgemein im Rahmen einer datenschutzrechtlichen Risikobewertung mit einzubeziehenden Szenarien und Folgen. Solche Risiken

„können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann,

wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren,

wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden,

wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen,

wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder

wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.“

Dieses „Potpourri“ an risiko- bzw. gefahrerhöhenden Umständen enthält aus der Perspektive des Art. 35 Abs. 3 DSGVO eine konkrete Aufgliederung des Begriffs der „persönlichen Aspekte“ und die – wenig überraschende – Bestätigung, dass die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 und 10 DSGVO „riskant“ ist. Ein bisschen „beißt“ sich dieser Erwägungsgrund allerdings mit der grundsätzlichen Einsicht, dass jede Verarbeitungshandlung ein Risiko für die Rechte und Freiheiten natürlicher Personen darstellt (s. auch Art. 32 DSGVO). Auch Erwägungsgrund 75 kann also eigentlich nicht die abschließende Auflistung sämtlicher risikoerhöhender Faktoren beinhalten (so ist er aber sprachlich formuliert), sondern nur die „Hauptkandidaten“ für eine Risiko- bzw. Gefahrerhöhung.

Die in Erwägungsgrund 75 aufgeführten gefahrerhöhenden Elemente führen nicht automatisch zum Vorliegen eines hohen Risikos. Sie zeigen aber Bereiche auf, die außerhalb der „insbesondere“-Szenarien in Art. 35 Abs. 1 und Abs. 3 DSGVO zusätzlich zu beleuchten sind. Zudem können die dort aufgeführten Elemente eine Richtschnur für eine „Standard-Risikobewertung“ unterhalb des hohen Risikos darstellen. Wir werden unten noch im Einzelnen auf die einzelnen Elemente zurückkommen.

- Die Datenschutzbehörden

Daneben hat der Gesetzgeber den Datenschutzbehörden aufgegeben, eine „Blacklist“ derjenigen Verarbeitungsvorgänge aufzustellen, für die eine Datenschutz-Folgenabschätzung durchgeführt werden muss (Art. 35 Abs. 4 DSGVO). Nun haben die deutsche DSK und viele Landesdatenschutzbeauftragte jeweils eigene Blacklists entwickelt, die sich auf den ersten Blick ähneln, auf den zweiten Blick aber teils erhebliche Unterschiede enthalten. Natürlich enthalten diese viele unbestimmte Rechtsbegriffe, insbesondere das Wort „umfangreich“, das man sich vom Gesetzgeber abgeschaut hat.

Diese Blacklists wiederum basieren nach den Angaben der Datenschutzbehörden auf dem Arbeitspapier („*working paper*“ – WP) 248 der Art.-29-Datenschutzgruppe aus dem Jahr 2017 (für die DSGVO bestätigt durch den Europäischen Datenschutzausschuss), welches (nicht-abschließend) folgende Kriterien für die Ermittlung eines hohen Risikos aufführt:

- Bewerten und Einstufen (Erstellen von Profilen und Prognosen, einschließlich der Einholung von Auskünften einer Kreditauskunftei)
- automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
- systematische Überwachung
- Verarbeitung vertraulicher Daten oder höchst persönlicher Daten
- Datenverarbeitung in großem Umfang
- Abgleichen oder Zusammenführen von Datensätzen in einer Weise, die über die vernünftigen Erwartungen des Betroffenen hinausgeht
- Verarbeitung von Daten zu schutzbedürftigen Betroffenen
- innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen und
- Fälle, in denen die Verarbeitung an sich die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert.

Auch hier liegen erhebliche Überschneidungen mit den in Art. 35 DSGVO aufgeführten Szenarien sowie mit den in Erwägungsgrund 75 aufgeführten Umständen vor, aber auch darüber hinausgehende Fälle, die sich mit dem Grundkonzept des Standard-Datenschutzmodells und seiner „Gewährleistungsziele“ erklären lassen. Das Besondere an den behördlichen Blacklists ist, dass hier nicht kritisiert werden kann, diese würden keine „richtige“ Konkretisierung des Gesetzes darstellen, da den Behörden von Art. 35 Abs. 4 DSGVO insoweit eine Art „Rechtssetzungskompetenz“ eingeräumt wird. Ob und in welchen inhaltlichen Grenzen das mit der dürren Gesetzesformulierung („*Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese*“) europarechtlich zulässig ist, soll hier nicht weiter hinterfragt werden.

Das besagte Arbeitspapier 248 geht davon aus, dass, wenn ein Verarbeitungsvorgang zwei dieser Kriterien erfüllt, der Verantwortliche „*in den meisten Fällen zu dem Schluss kommen*“ muss, dass eine Datenschutz-Folgenabschätzung notwendig ist. Es könne jedoch auch „*in*

einigen Fällen“ vorkommen, dass schon bei Vorliegen nur eines Kriteriums eine Datenschutz-Folgenabschätzung notwendig sei. Umgekehrt könne es vorkommen, dass ein Verantwortlicher einen mehrere Kriterien erfüllenden Fall nicht als maßgeblichen Vorgang mit hohem Risiko bewertet; in diesem Fall sei die Nichtdurchführung einer Datenschutz-Folgenabschätzung zu begründen und zu dokumentieren und der Standpunkt des Datenschutzbeauftragten sei dabei mit einzubeziehen bzw. festzuhalten. Es handelt sich daher eher um eine grobe Richtschnur als um ein präzises Indikatoren-System.

Es mag also durchaus einige Fälle geben, in denen die vom Gesetz und den Datenschutzbehörden definierten Szenarien zweifelsfrei vorliegen. Die Mehrzahl der Fälle wird aber unterhalb dieser „Eindeutigkeits-Schwelle“ liegen, und aus den genannten Szenarien lässt sich keine definierte „Untergrenze“ für die Annahme eines hohen Risikos herleiten.

Das Kurzpapier Nr. 5 der Datenschutzkonferenz kündigt ein weiteres Kurzpapier zur Schwellwertanalyse an, aber bislang gibt es hierzu keine weitere (ohnehin nur unverbindliche) Interpretationshilfe der deutschen Datenschutzbehörden.

➢ Die Checklisten

Auf dem Markt kursieren nun Checklisten, welche die verschiedenen oben aufgeführten Kriterien zu konsolidieren und konkreter zu formulieren versuchen. Hiernach kann sich ein hohes Risiko (typisiert) durch verschiedene Faktoren bzw. Gefährdungspotenziale ergeben, die sich an die oben aufgeführten Rechtsquellen Gesetz und behördliche Vorgaben anlehnen. Allerdings zeigt sich auch hier – wen wundert’s? –, dass sich dadurch keine große Verbesserung in Sachen Beurteilungsspielraum ergibt:

- *Bei der Verarbeitung soll eine neue, bisher noch nicht in einer Datenschutz-Folgenabschätzung untersuchte Informations- und Kommunikationstechnik eingesetzt werden.*
  Das Kriterium stammt aus dem Szenario der „Verwendung neuer Technologien“ in Art. 35 Abs. 1 DSGVO. Wenn dies allerdings für jeden Verantwortlichen separat beurteilt werden müsste, dann müsste für jedes neue IT-System bei jedem Verantwortlichen zumindest eine Datenschutz-Folgenabschätzung durchgeführt werden. Wenn dies hingegen für die Summe aller Verantwortlichen (in Deutschland? in der EU?) gelten sollte, dann müsste jeder Verantwortliche wissen, was die anderen Verantwortlichen so bisher abgeschätzt haben – dazu gibt es aber keine Datenbank.

- *Bei der Verarbeitung soll eine hochkomplexe und stark miteinander vernetzte Informations- und Kommunikationstechnik eingesetzt werden.*
  Das Kriterium kann aus dem WP 248 („Datenverarbeitung in großem Umfang") abgeleitet werden. Die Bedingungen „hochkomplex" und „stark vernetzt" setzen einen Maßstab der „normalkomplexen" bzw. „normal vernetzten" IT-Systeme voraus. Das ist aber nirgends definiert.

- *Bei der Verarbeitung soll eine große Menge personenbezogener Daten verarbeitet werden.*
  Das Kriterium stammt aus dem WP 248 und ist auch in Erwägungsgrund 75 genannt. Was eine „große" Zahl ist, bleibt natürlich unklar. Geht es um hunderte Datensätze? Tausende? Millionen?

- *Von der Verarbeitung ist eine große Anzahl von Personen betroffen.*
  Auch dieses Kriterium stammt aus dem WP 248 sowie aus Erwägungsgrund 75. Hier stellt sich die gleiche Frage wie bei der Menge der personenbezogenen Daten. Durch die Trennung in zwei Kriterien kann es immerhin sein, dass eine große Menge personenbezogener Daten einer kleinen Anzahl von Personen ebenso wie eine kleine Menge personenbezogener Daten einer großen Anzahl von Personen relevant wird.

- *Die Verarbeitung dient der systematischen und umfangreichen großflächigen Überwachung im öffentlichen Raum.*
  Dieses Kriterium setzt ein gesetzliches Regelbeispiel um (Art. 35 Abs. 3 lit. c DSGVO), konkretisiert („umfangreich") dies aber nicht.

- *Die Verarbeitung soll teilweise oder vollständig (z. B. hinsichtlich Speicherung, Datensicherung oder Fernwartung) in einem Drittland durchgeführt werden, welches gemäß der Rechtsauffassung der EU-Kommission über kein angemessenes Datenschutzniveau verfügt.*
  Dieses Kriterium findet sich z. B. in der Blacklist des Bayerischen Landesamts für Datenschutzaufsicht im Rahmen der Datenschutz-Folgenabschätzung, jedoch nicht generell (Drittlandsverarbeitung), sondern qualifiziert als *„Umfangreiche und innovative Verarbeitung vertraulicher oder höchstpersönlicher Daten in Drittländern"*. Das eigentlich qualifizierende Kriterium ist hier also nicht die Drittlandsverarbeitung als solche, sondern Innovation (Art. 35 Abs. 1 DSGVO) bzw. umfangreiche Verarbeitung (WP 248). Die Formulierung „teilweise oder vollständig" führt im Umkehrschluss

dazu, dass nur für Verarbeitungen, die in der EU oder in sicheren Drittländern durchgeführt werden, keine Datenschutz-Folgenabschätzung notwendig ist. Somit wäre schon bei allen personenbezogenen Daten auf Websites, die aus unsicheren Drittländern heraus aufgerufen werden können, eine Datenschutz-Folgenabschätzung durchzuführen? Dann müsste – wegen der Impressumspflichten, die zur Veröffentlichung zumindest der Namen von Organen zwingen – wohl jeder Website-Betreiber eine Datenschutz-Folgenabschätzung durchführen.

- *Die Verarbeitung ermöglicht eine umfassende und mit dem ursprünglichen Zweck der Datenerhebung nicht unmittelbar vereinbare Verknüpfung und Auswertung der gespeicherten Daten unter Berücksichtigung von Art. 6 Abs. 4 DSGVO.*
  Dieses Kriterium geht ebenfalls auf das WP 248 zurück. Es kann in dieser Formulierung („ermöglicht") für jedes Datum einschlägig sein, das aufgrund gesetzlicher Aufbewahrungspflichten – die mit dem ursprünglichen Erhebungszweck nichts zu tun haben – weiter gespeichert wird und natürlich auch eine Verknüpfung mit anderen Daten und eine Auswertung ermöglicht. Ob diese Verknüpfung und Auswertung dann tatsächlich stattfindet, ist schon nicht mehr relevant.

- *Für die Verarbeitung sollen zahlreiche Auftragsverarbeiter eingesetzt werden, die über einen Fernwartungszugang verfügen.*
  Die Herleitung dieses – formalen, nicht auf den Dateninhalt abstellenden – Kriteriums ist unklar. Abgesehen davon, dass „zahlreich" genauso undefiniert wie „umfangreich" ist, stellt sich die Frage, was an einem ordentlichen Fernwartungszugang mit korrekter Auftragsverarbeitungsvereinbarung so viel schlechter sein soll als wenn die gesamte IT an einen Auftragsverarbeiter ausgelagert wird (Outsourcing), der dann nur nicht „fernwartet", aber alles „hat".

- *Die Verarbeitung ermöglicht den Betroffenen keinerlei Form einer unmittelbaren Kontrolle ihrer Daten (z. B. vom Betroffenen aufrufbare Anzeige der über ihn gespeicherten Daten) oder erschwert den Betroffenen die Ausübung ihrer Rechte entgegen der Vorgabe aus Art. 12 Abs. 2 DSGVO.*
  Dieses Kriterium kann dem WP 248 zugeordnet werden. Abgesehen davon aber, dass Art. 12 Abs. 2 DSGVO davon spricht, dass die Ausübung der Betroffenenrechte vom Verantwortlichen „erleichtert" werden soll – was immer das im Einzelnen heißt –, geben die wenigsten Systeme den Betroffenen eine unmittelbare Kontrolle über ihre Daten. Andersherum: Die Fälle, in denen die Betroffenen eine unmittelbare Kontrolle über ihre Daten haben, sind in der Praxis kaum mehr als die Fälle, in denen ein Kunde

in einem Webshop oder bei einem sonstigen Online-Anbieter seine eigenen (Stamm-) Daten ändern kann. Welcher Betroffene, dessen Daten in einem CRM-, einem ERP- oder einem DMS-System gespeichert sind, kann diese selbst ändern? Welcher Beschäftigte hat die über ihn in einer elektronischen oder physischen Personalakte gespeicherten Daten „unter unmittelbarer Kontrolle"? Welcher Absender einer E-Mail hat noch die Hand auf den Informationen, nachdem diese an den Empfänger verschickt, von diesem ggf. weitergeleitet, ausgedruckt, archiviert wurde?

- *Die Verarbeitung soll zu einer automatisierten Entscheidungsfindung führen, die gegenüber dem Betroffenen eine rechtliche Wirkung entfaltet oder den Betroffenen in ähnlicher Weise erheblich beeinträchtigt, ohne dass der Betroffene seinen Standpunkt zur Anfechtung der Entscheidung vortragen kann.*
  Dieses Kriterium stammt aus Art. 35 Abs. 3 lit. a DSGVO, ist aber nicht – wie dort – auf eine *„systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen"* beschränkt. Auch hier ist es zumindest die Unklarheit in der Begrifflichkeit („erheblich beeinträchtigt"), die der praktischen Anwendung entgegensteht. Zudem stellt das Entfalten einer rechtlichen Wirkung gegenüber dem Betroffenen nicht immer eine „erhebliche Beeinträchtigung" des Betroffenen dar, d. h. die „in ähnlicher Weise"-Formulierung ist – auch im Gesetzestext – eigentlich verfehlt.

- *Die Verarbeitung kann die Betroffenen an der Nutzung einer Dienstleistung bzw. an der Durchführung eines Vertrags hindern.*
  Auch dieses – aus dem WP 248 abgeleitete – Kriterium basiert letztlich auf einer automatisierten Entscheidungsfindung, die einen Betroffenen „aussperrt". Die Formulierung unterscheidet aber nicht danach, ob der Betroffene (aus rechtlicher Sicht) die Dienstleistung überhaupt nutzen bzw. einen Vertrag durchführen können muss. Die datenschutzrechtliche Sichtweise kann hier durchaus mit dem Grundsatz der Vertragsfreiheit kollidieren: Außerhalb besonderer Bereiche (Monopole etc.) darf jeder Verkehrsteilnehmer selbst entscheiden, mit wem er einen Vertrag abschließt und mit wem nicht, und er kann (aus zivilrechtlicher Sicht) diese Entscheidung natürlich auch einem System überlassen. Dies ist allerdings ein Bereich – die „unmittelbare Drittwirkung der Grundrechte" –, der sich in Zukunft weiter verändern wird, indem die Verantwortlichen (wie traditionell ein Gesetzgeber oder die Verwaltung) verschiedene Grundrechte gegeneinander abwägen müssen. Im Übrigen überschneiden sich in diesem Kriterium Betroffenenrechte (Art. 22 DSGVO) und risikoerhöhende Faktoren: Die

Gefahr, dass andere Betroffenenrechte (z. B. die Löschung) nicht erfüllt werden, begründet auch sonst nicht pauschal die Annahme eines erhöhten Risikos der Verarbeitungshandlung selbst.

- *Die unbefugte Verwendung der gespeicherten Daten ermöglicht eine Diskriminierung des Betroffenen.*
  Dieses und die folgenden Kriterien wurden aus Erwägungsgrund 75 abgeleitet. Sie stellen dort einen in die Risikobewertung einzustellenden Faktor dar, den man auch als „risikoerhöhend" interpretieren kann (auch wenn Erwägungsgrund 75 nicht ausdrücklich von Risikoerhöhung spricht). Auch hier findet sich wieder das gefährliche „Ermöglichen" als einziges Kriterium. Viele Daten „ermöglichen" eine Diskriminierung, man denke nur an Nachnamen, und das dann natürlich auch in Fällen der unbefugten Verwendung.

- *Die gespeicherten Daten können von einem Unbefugten für Identitätsmissbrauch oder Identitätsbetrug verwendet werden.*
  Beim Identitätsdiebstahl (besser, und auch im Folgenden, Identitätsmissbrauch) wird neben dem Namen eine Reihe persönlicher Daten wie beispielsweise Geburtsdatum, Anschrift, Führerschein- oder Sozialversicherungsnummern, Bankkonto- oder Kreditkartennummern genutzt, um die Feststellung der tatsächlichen eigenen Identität (des Missbrauchenden) zu umgehen oder diese zu verfälschen. Je mehr zueinander passende Daten der Missbrauchende hat, desto sicherer wird ihm die Vorspiegelung gelingen.

  Dies bedeutet jedoch nicht, dass bereits ein Abzug „irgendwelcher" Daten, im Extremfall nur eines (Nach-) Namens, einen Identitätsmissbrauch ermöglichen würde. Wäre dies der Fall, so wäre allein die Verarbeitung von (Nach-) Namen ein Fall des hohen Verarbeitungsrisikos. Vielmehr müssen die Datenkategorien in ihrer Kombination geeignet sein, sich einem Dritten bzw. einem IT-System gegenüber zu autorisieren. Es ist offen, ab welcher Kombination von Datenkategorien von „identitätsmissbrauchsfähigen" Daten gesprochen werden kann (in der strafrechtlichen Terminologie die „Tiefe und Ausdifferenzierung der Legende"); eine gesicherte (Mindest-) Definition besteht nicht. Veröffentlichte Sicherheitsberichte bezeichnen etwa die amerikanische Social Security Number als „wertvolle Identitätsinformation".

Grundsätzlich kann aufgrund des Vergleichs mit den anderen Kategorien eines potenziell hohen Risikos der Datenverarbeitung davon ausgegangen werden, dass zumindest Name, (private) postalische Adresse und (private) Bankverbindung abgezogen werden müssen, um einen Identitätsdiebstahl (z. B. im Wege eines Kaufs auf Rechnung) zu ermöglichen. Selbst dies würde aber schon bedeuten, dass jeder Verarbeitung von Beschäftigtendaten ein hohes Risiko immanent ist, das eine Datenschutz-Folgenabschätzung erforderlich macht. Zwar gibt es einen gut dokumentierten Fall (2009), in denen ein finanzieller und Ruf-Schaden des Opfers (Betroffenen) schon mit Name und Geburtsdatum erzielt wurde, aber einerseits ist zweifelhaft, ob heutzutage mit einer solchen Kombination bereits ein (finanzieller) Schaden erzeugt werden kann, und andererseits würde die Annahme eines „hohen Risikos" bereits aufgrund der Speicherung dieser Datenkategorien ein allgemeines Lebensrisiko, das stets – auch bei noch so rudimentären Datensätzen und ohne Verfügungsmacht über sensible Daten – vorliegen kann, zur höchsten datenschutzrechtlichen Risikokategorie erheben.

- *Eine unbefugte Verwendung der gespeicherten Daten kann für den Betroffenen zu einem finanziellen Verlust führen.*
  Ein „finanzieller Verlust" im Sinne dieses Kriteriums kann wohl kaum in irgendeinem (Kosten-) Aufwand des Betroffenen für die Abwehr unberechtigter Behauptungen, Rufschädigungen oder eines Identitätsmissbrauchs liegen, denn ein solcher Aufwand kann mit jeder behaupteten Rechtsverletzung – auch Bagatellverletzung – einhergehen. Vielmehr muss dem Betroffenen, damit das Vorliegen eines hohen Risiko gerechtfertigt sein kann, ein nicht nur unerheblicher Schaden im materiellen Sinne zugefügt werden, etwa der (zivilrechtlich endgültige) Verlust eines Anspruchs, der Verlust von Geld oder Vermögensgegenständen als direkte Folge eines Identitätsmissbrauchs oder der (nachweisliche) Verlust der Möglichkeit des Abschlusses eines gewinnbringenden Vertrages durch eine Rufschädigung etc.

- *Eine unbefugte Verwendung der gespeicherten Daten kann für den Betroffenen zu einer Rufschädigung führen.*
  Der Begriff „Rufschädigung" ist wohl ebenso schillernd wie der des Identitätsbetruges. Auch hier muss, wie bei den vorstehenden Kriterien, eine gewisse Erheblichkeit der Rufschädigung vorliegen, denn im Prinzip kann mit jedem personenbezogenen Datum irgendeine Form von Rufschädigung verursacht werden.

- *Eine unbefugte Einsichtnahme in die gespeicherten Daten verletzt ein bestehendes Berufsgeheimnis, dem die personenbezogenen Daten unterliegen.*
  Damit wäre die Datenverarbeitung sämtlicher Berufsgeheimnisträger – etwa auch einzeln praktizierende Ärzte oder Steuerberater – als „potenziell gefahrgeneigt" einzustufen. Das bedeutet nicht unmittelbar, dass eine Datenschutz-Folgenabschätzung durchzuführen ist, steht aber für einzelne Selbstständige in gewissem Widerspruch zum Erwägungsgrund 91, wonach in diesem Fall nicht von einer „umfangreichen" Verarbeitung auszugehen ist und eine Datenschutz-Folgenabschätzung „nicht zwingend vorgeschrieben sein" sollte.

- *Die Pseudonymisierung gespeicherter Daten kann von einem Unbefugten nach Zugriff auf die gespeicherten Daten aufgehoben werden.*
  Dies wäre immer dann der Fall, wenn ein Verantwortlicher personenbezogene Daten pseudonymisiert hat und die Zuordnungsinformation an anderer Stelle aufbewahrt als die Daten selbst – dann kann der unbefugte Zugriff auf die Zuordnungsinformation die Pseudonymisierung aufheben. Könnte man dann die Gefahrerhöhung dadurch abwenden, dass man nicht pseudonymisiert?

- *Eine unbefugte Verwendung der gespeicherten Daten kann für den Betroffenen zu einem erheblichen wirtschaftlichen Nachteil führen.*
  Es ist schon unklar, was der Unterschied zwischen einem finanziellen Verlust (s. o.) und einem erheblichen wirtschaftlichen Nachteil ist.

- *Eine unbefugte Verwendung der gespeicherten Daten kann für den Betroffenen zu einem erheblichen gesellschaftlichen Nachteil führen.*
  Auch hier ist unklar, was ein erheblicher gesellschaftlicher Nachteil in Abgrenzung zu einer Rufschädigung sein soll.

Man kann an dieser Stelle zuerst einmal resümieren, dass auch derartige Listen – wie der Gesetzestext auch – mehr Fragen aufwerfen, als sie beantworten. Weiter muss sehr genau geprüft werden, ob solche Listen nicht in einzelnen Punkten über die gesetzlichen oder behördlichen Vorgaben hinausschießen – und damit übermäßigen Aufwand generieren – oder im Einzelfall sogar im Widerspruch zu Aussagen der Datenschutzbehörden an anderer Stelle stehen. So kann man sich leicht ausmalen, dass die obigen Kriterien bei der Verarbeitung von Beschäftigtendaten eines Unternehmens beinahe immer zur Annahme einer hohen Risikos führen werden, an die sich die Durchführung einer Datenschutz-Folgenabschätzung anschließt. Gleichwohl soll bei der typischen Verarbeitung von Beschäftigtendaten zur

Durchführung von Beschäftigungsverhältnissen nach Ansicht des Bayerischen Landesamts für Datenschutzaufsicht gerade keine Datenschutz-Folgenabschätzung durchzuführen sein. In ihren „FAQs" führt die Behörde aus, dass *„in der Regel bei Verarbeitung von Personaldaten keine DSFA durchzuführen ist. Eine Ausnahme stellen ggf. umfangreiche zentrale Personalverwaltungen in (internationalen) Konzernstrukturen dar"*. Da ist es übrigens wieder – das unbestimmte Wort „umfangreich". Die Aussage der Behörde ist insoweit nachvollziehbar, als die Notwendigkeit einer Datenschutz-Folgenabschätzung bei jeder Verarbeitung von Beschäftigtendaten jeden Arbeitgeber in der EU betreffen würde. Hätte der DSGVO- oder BDSG-Gesetzgeber eine solche Notwendigkeit bei jedem Unternehmen gesehen, so hätte dies in dieser Pauschalität gesetzlich oder – über Art. 35 Abs. 4 DSGVO – behördlich festgelegt werden können und müssen.

Allerdings soll – so die Checkliste – das Vorliegen eines des oben aufgeführten Kriterien noch nicht zu einem hohen Risiko und damit zur Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung führen. Das leuchtet unmittelbar ein, denn die Kriterien können, wie oben gezeigt, durchaus auch „Niedrigrisiko-Verarbeitungssituationen" erfassen. Vielmehr liegt, wenn eine oder mehrere Kriterien erfüllt sind, zunächst nur (im Grunde müsste man sagen: allenfalls) ein „potenziell hohes Risiko" (also ein Indiz) vor, das – wie auch bei einer „normalen" Risikobeurteilung – nur dann ein hohes Risiko sein soll, wenn dessen Eintrittswahrscheinlichkeit hoch ist. Auf die diesbezüglich vorgeschlagenen weiteren (typisierten) Kriterien zur Bemessung der Eintrittswahrscheinlichkeit soll hier nicht eingegangen werden. Stattdessen schwenken wir an dieser Stelle auf die „normale" Risikobeurteilung nach der Maßgabe des Kurzpapiers 18 der DSK um, die ebenfalls die Eintrittswahrscheinlichkeit misst, aber nicht auf Basis typisierter Szenarien, sondern auf der Basis konkreter Szenarien, aber typisierter Ursachen und typisierter Indikatoren für die Messung der Schwere des (möglichen) Schadens.

➢ Die „normale" Risikobeurteilung

Bei negativem Ergebnis einer Schwellwert-Analyse mit typisierten Kriterien ist eine „gewöhnliche" Risikoanalyse (das Kurzpapier 18 der DSK spricht insoweit von einem „vereinfachten Verfahren") durchzuführen. In deren Rahmen ist zu untersuchen, durch welche Handlungen oder Umstände es zum Eintritt schädigender Ereignisse (DSGVO-Verstößen) kommen kann, die dann in einen konkreten Schaden münden (Szenarienanalyse). Basierend auf der Analyse möglicher Szenarien ist dann die Eintrittswahrscheinlichkeit des Szenarios und des Schadens (bzw. die Schwere eines wahrscheinlichen Schadens) zu schätzen.

Dabei sind naturgemäß Überschneidungen mit den Inhalten der Schwellwert-Analyse im Kontext einer (etwaigen) Datenschutz-Folgenabschätzung möglich. Eine Schwellwert-Analyse dient ja dem Zweck, anhand von typisierten Kriterien festzustellen, ob ein „hohes Risiko" vorliegt. Eine gewöhnliche Risikoanalyse unterhalb dieser Schwelle anhand von konkreten Szenarien sollte dann besser nicht zu dem Ergebnis kommen, dass doch ein „hohes Risiko" vorliegt. Also sollte die Schwellwert-Analyse insoweit zum selben Ergebnis kommen wie die gewöhnliche Risikoanalyse – auch wenn für beide andere Methoden angewandt werden –, sonst läuft etwas falsch. Aber auch die gewöhnliche Risikoanalyse kann dann eigentlich nur noch zwischen „normalem Risiko" und eventuell noch einem „Nur-Restrisiko" (Niedrigrisiko) der Verarbeitung unterscheiden, soweit man das Ergebnis nicht – was zumindest in gängigen Checklisten nicht der Fall ist – feingranularer in weitere Risiko-Stufen oder Risiko-Prozentwerte „aufdröselt". Ob dieses Vorgehen eines solchen datenschutzrechtlichen Risiko-„*key performance index*" als „kontextlose Zahl" überhaupt sinnvoll ist, ist am Ende der Übung noch zu hinterfragen.

Nach dem Standard-Datenschutzmodell ist im Rahmen der Planung und Spezifikation (inkl. Risikoanalyse) die Erarbeitung von „Usecases" notwendig, um daraus ein Angreifermodell für die Verarbeitung bilden zu können, in denen beteiligte Akteure befugt und unbefugt (als Angreifer) auf Daten zugreifen könnten (Baustein M41.07 des Standard-Datenschutzmodells). Anhand der Usecases und der Akteure können alle relevanten Komponenten erkannt werden, deren Funktionieren datenschutzrechtlich überprüft werden muss, um zum Schluss dann die Risiken der Betroffenen durch den geplanten Betrieb der Verarbeitung rechtlich beurteilen zu können. Das Risiko für die Rechte und Freiheiten Betroffener durch die Verarbeitung ist zunächst für den Fall zu bestimmen, dass die Daten zum vorgesehen Zweck verarbeitet werden und noch keine zusätzlichen technischen und organisatorischen Maßnahmen getroffen werden (M41.08). Dieses Risiko entspricht dann dem Schutzbedarf der Betroffenen. Dies bedeutet: Es geht bei der gewöhnlichen Risikoanalyse in erster Linie darum, die „Risikoszenarien" im Rahmen der konkreten Umstände des Einzelfalles zu identifizieren und durch gezielte Maßnahmen das Risiko abzuschirmen. Schon dies zeigt, dass die Ermittlung eines „Gesamtrisikos" als „normal" oder „Nur-Restrisiko" für sich genommen wenig aussagt, denn aus dieser „binären" Aussage allein lassen sich keine konkreten Maßnahmen für die konkrete Situation ableiten.

Kommen wir wieder zurück zum „vereinfachten Verfahren" und der Szenarienanalyse. Handlungen oder Umstände im Sinne des Kurzpapiers 18 der DSK sind insbesondere, auch durch höhere Gewalt oder technische Fehlfunktionen,

- der Abzug der personenbezogenen Daten durch und die Übermittlung an Unbefugte (inkl. Cyberkriminelle, unbefugte staatliche Stellen, Kommunikationspartner, Empfänger von über automatische Schnittstellen übermittelte Daten, aber auch unbefugte Beschäftigte bzw. Beschäftigte, die sich durch Zweckdurchbrechung zum Verantwortlichen „aufschwingen“) sowie die anschließende „Ausbeutung“ dieser Daten auch durch Verknüpfung der Daten untereinander sowie mit anderen Daten (inkl. Profilbildung),
- die zufällige Vernichtung von Daten,
- der Ausfall oder Einschränkungen von vorgesehenen Prozessen,
- die unbeabsichtigte oder vorsätzliche unbefugte Veränderung der Daten,
- die mutwillige Veränderung der Zweckbindung,
- die weitere (datenschutzwidrige) Speicherung von Daten, welche die vorstehenden Handlungen oder Umstände ermöglicht.

Man kann das zu folgenden Fallgruppen – jeweils unter Angabe der betroffenen Schutzziele des Standard-Datenschutzmodells – umformulieren:

- Unbefugter Datenabzug (Kenntnisnahme durch einen unternehmensinternen oder externen Unbefugten) – Vertraulichkeit –,
- Unbefugte Verkettung (Zusammenführung mit anderen Daten über den Betroffenen, insbesondere durch einen unbefugten Kenntnisnehmer) – Nichtverkettung –,
- Unbefugte Verwendung (Aktionen gegen den Dritten unter Zuhilfenahme der Daten, insbesondere durch einen unbefugten Kenntnisnehmer) – Intervenierbarkeit, Transparenz, Vertraulichkeit –,
- Unbefugte Vernichtung/Veränderung (absichtlich oder unabsichtlich, jeweils mit der Folge, dass keine inhaltlich richtigen Daten mehr zur Verfügung stehen), wobei dies auch nur temporär sein kann (Einschränkung der Verfügbarkeit) – Verfügbarkeit, Integrität –,
- Unbefugte Fortspeicherung (Nichtlöschung durch den Verantwortlichen trotz gebotener Löschung) – Datenminimierung, Vertraulichkeit, Intervenierbarkeit – sowie
- (Übermäßige) Abschirmung der Daten gegenüber dem Betroffenen (der Betroffene kann die Daten nicht genau einsehen bzw. weiß nicht, welche personenbezogenen Daten über ihn dem Verantwortlichen genau vorliegen) – Transparenz, Intervenierbarkeit.

„Unbefugte“ in diesem Sinne können Befugte (Mitarbeiter des Verantwortlichen) sein, die ihre Befugnisse (vorsätzlich oder fahrlässig) überschreiten, aber natürlich auch Dritte, die sich – meist vorsätzlich bzw. böswillig – Zugriff auf die Daten verschaffen. Schließlich, und

darauf ist unten noch zurückzukommen, kann „unbefugt“ auch „einfach so“ meinen, d. h. ohne entsprechende (befugte) Handlung.

Relevante Schäden, die nach dem Kurzpapier 18 der DSK aus solchen Handlungen oder Umständen resultieren können und in die Risikobewertung einzubeziehen sind, sind – neben dem Eingriff in das Grundrecht auf Datenschutz (Art. 8 Abs. 1 der EU-Grundrechtecharta) als solchem – insbesondere:

- Diskriminierung oder Rufschädigung des Betroffenen (einschließlich gesellschaftlicher Nachteile),
- Profilerstellung oder Profilnutzung durch eine Bewertung persönlicher Aspekte (Profilbildung),
- Identitätsmissbrauch oder Identitätsbetrug,
- finanzielle Verluste bzw. wirtschaftliche Nachteile des Betroffenen,
- Erschwerung der Ausübung von Rechten und Freiheiten (einschließlich Belästigung des Betroffenen) sowie
- Verhinderung der Kontrolle (über die Daten) seitens der betroffenen Person selbst.

Der Kern dieser Form der Risikobewertung ist damit die Formulierung hypothetischer Szenarien im konkreten „Setting“ des konkreten Verantwortlichen (und insbesondere seiner IT-Landschaft) sowie die Beantwortung der Frage, ob in dem jeweiligen Szenario der Eintritt eines Schadens der oben genannten Art möglich ist. Die Huber AG müsste sich also im Ausgangsfall jeweils überlegen, ob bzw. wie ein unbefugter Datenabzug beispielsweise aus einem IT-System, das Personalaktendaten verarbeitet, möglich wäre. Ist etwa ein Gesamt-Datenbank-Abzug durch einen „Dump“ bzw. Excel-Export einfach möglich, wäre das Szenario schon im Ansatz ein anderes, als wenn letztlich aufgrund der Struktur der eingesetzten Software nur ein mühsames Kopieren (oder Abfotografieren) einzelner Bildschirm- bzw. Feldinhalt möglich wäre. Führt der Datenabzug – also die Kenntnisnahme durch den Unbefugten – für sich genommen noch nicht zu einem Schaden (üblicherweise bedarf es einer „Verwertung“ der gewonnenen Erkenntnisse), so kann das Szenario in einem weiteren Szenario der „unbefugten Verwendung“ dahingehend ausgedehnt werden, wie der Betroffene mit den im Rahmen des Abzugs „erbeuteten“ Daten dann „angegangen“ – also beschädigt – werden kann. Das kann lediglich eine Belästigung des Betroffenen mit unerwünschter Werbung oder eine Profilerstellung mit der Absicht des Identitätsmissbrauchs sein. Eine unbefugte Veränderung z. B. einer Kontoverbindung kann aber auch zu einer Fehlüberweisung und damit einem (vorläufigen) finanziellen Schaden des Betroffenen führen.

Nur am Rand: Das Szenario „manipulativer Austausch des Betroffenen“ wird bislang in der Praxis wenig beleuchtet, obwohl damit Informationsströme umgeleitet oder – noch gefährlicher – unbemerkt durch einen Angreifer hindurchgeschleust werden können („*man in the middle*“-Angriff). Würde etwa die E-Mail-Adresse eines Ansprechpartners eines Geschäftskunden der Huber AG durch eine andere (unternehmensfremde) E-Mail-Adresse ausgetauscht, so könnten personenbezogene Daten, die nicht für diesen (dritten) Adressaten bestimmt sind, an diesen gelangen. Die E-Mail des Mitarbeiters des Geschäftskunden der Huber AG, der Maier GmbH, könnte von „p.maier@maier-gmbh.com“ in die um einen Buchstaben unterschiedliche „p.maier@maier-gmbl.com“ geändert werden. Die an diese E-Mail-Adresse gesendeten E-Mails könnten damit entweder dem eigentlichen Adressaten vorenthalten werden oder an diesen weitergeleitet werden (ebenso wie die Rückantworten), sodass die Veränderung des Datums zunächst nicht auffällt. Auch diese Weise können relevante Informationen abfließen und neben einem Kontrollverlust auch zu einer Vertiefung der Möglichkeit eines Identitätsmissbrauchs führen (man denke nur an die sog. „CEO fraud“-Fälle).

Die Eintrittswahrscheinlichkeit der Ursache des Szenarios (also warum etwa ein Datenabzug passiert) und die Schwere des Schadens (also wie schwerwiegend der etwa durch eine unbefugte Verwendung ausgelöste Schaden für den Betroffenen ausfallen kann) spielen hier zunächst keine Rolle. Es geht im ersten Schritt nur darum, dass ein bestimmtes Szenario und ein daraus resultierender Schaden möglich sind. Schon dies ist nicht trivial: Was (etwa im Bereich der Verkettung verschiedener Umstände) der eine als möglich ansehen mag, wird jemand anderes als „völlig praxisfern“ ansehen und deshalb gar nicht weiter untersuchen. Ist es ein taugliches Szenario, dass ein „Täter“ Daten abzieht und auf einer MicroSD-Karte gespeichert im Mund aus dem Gebäude bringt, um eine Leibesvisitation beim Verlassen des Gebäudes unentdeckt zu überstehen, wie Edward Snowden dies von seinem NSA-Datenabzug berichtete? Ist es ein taugliches Szenario, dass Trojaner über Datenträger auf Systeme eingeschleust werden, die nicht selbst mit dem Internet verbunden sind? Ist es ein taugliches Szenario, dass – wie oben beschrieben – ein Beschäftigter mit entsprechender Berechtigung böswillig eine andere E-Mail-Adresse in einem CRM-Programm hinterlegt, um an den entsprechenden Betroffenen gesandte E-Mails (z. B. mit Rabattcodes) abzufangen? Man kann all dies auf die Ebene der Eintrittswahrscheinlichkeit verschieben – dann wird man aber sehr viele Szenarien zu bewerten haben.

Für jedes der so ermittelten Szenarien – bestehend aus Handlungen bzw. Umständen und möglichen Schäden – sind Eintrittswahrscheinlichkeit und Schwere des Schadens zu schätzen. Hierfür können die vier Größenordnungen „geringfügig“, „überschaubar“, „substanziell“ und „groß“ verwendet werden, wobei diese eigentlich noch um die Größenordnung

„keine erhebliche Wahrscheinlichkeit“ (d. h. es liegt lediglich ein insignifikantes – prinzipiell nie ganz auszuschließendes – Restrisiko vor) ergänzt werden könnte. Im Bereich der Schwere ist beispielsweise zu beurteilen, wie schwerwiegend die möglichen negativen Folgen für die Lebensführung betroffener Personen einzustufen sind. Bei immateriellen Schäden (z. B. Rufschädigung) muss – nach Erwägungsgrund 76 zur DSGVO auf Basis (welcher?) „objektiver Kriterien“ – beurteilt werden, als wie schwerwiegend die möglichen negativen Folgen für die Lebensführung der betroffenen Personen einzustufen sind. Existieren mehrere Szenarien, die zum selben Schaden führen können, summieren sich Eintrittswahrscheinlichkeiten. Letzteres kann allerdings in der Praxis durchaus zu unplausiblen, „monströsen“ Ergebnissen führen.

Die Eintrittswahrscheinlichkeit der ermittelten Szenarien ist bezüglich des auslösenden Ereignisses (Handlung bzw. Umstand) insbesondere anhand folgender Ursachen zu bemessen:

- unzureichende Vorkehrungen beim Verantwortlichen (Nichtexistenz von technischen und organisatorischen Maßnahmen), wobei es hierbei nicht um mangelhafte IT-Sicherheit geht, die erst im Punkt „technische Fehlfunktionen“ relevant wird,
- sorgloser Umgang durch Beschäftigte (fahrlässiges Handeln),
- technische Fehlfunktionen (technisches Versagen, mangelhafte IT-Sicherheit) und
- „Ausspähung“ bzw. Handeln mit „krimineller Energie“ durch unternehmensinterne oder durch externe Dritte (vorsätzliches Handeln).

Dabei ist zu berücksichtigen, dass bei der gesamten Risikobeurteilung, also bis zur Ermittlung eines „Gesamtrisikos“ der Verarbeitung, ein Zustand ohne diejenigen weiteren (risikosenkenden) technischen und organisatorischen Maßnahmen unterstellt wird, die sich erst infolge der Risikobeurteilung als notwendig bzw. verhältnismäßig erweisen. Es wird also (nur) der Zustand der technischen und organisatorischen Maßnahmen, wie er sich zum Zeitpunkt der Risikobeurteilung darstellt, berücksichtigt. Vor diesem Hintergrund deckt die Fallgruppe „Nichtexistenz von technischen und organisatorischen Maßnahmen“ ausschließlich den Status Quo ab, ohne dass die Elemente der anderen Fallgruppen (wie vorsätzliches Handeln etc.) hinzutreten. In dieser Fallgruppe geschieht demnach eine Datenschutzverletzung „einfach so“ im gewöhnlichen Geschäftsgang bzw. im Rahmen des gewöhnliches Prozesses aufgrund der Abwesenheit technischer und organisatorischer Maßnahmen, ohne dass fahrlässiges oder vorsätzliches Handeln von Mitarbeitern oder Dritten, technisches Versagen oder mangelhafte IT-Sicherheitsmaßnahmen unterstellt werden. Eine signifikante Eintrittswahrscheinlichkeit in dieser Fallgruppe wäre demnach insbesondere Folge eines datenschutzrechtlich fehlerhaften oder „gefährlichen“ Programm-Designs, welches z. B. dazu führt, dass personenbezogene Daten (datenschutzwidrig) übermittelt, veröffentlicht oder

nicht gelöscht werden (s. auch oben Fall 36). Durch diese „Hintertür“ würden somit auch Aspekte von *„privacy by design“* bzw. *„privacy by default“* in die Risikobewertung einfließen: Softwareprodukte, die „datenschutzunfreundlich“ strukturiert oder parametrisiert wurden, würden bereits in dieser „Basis“-Fallgruppe zu einem erheblichen Risiko führen können.

Neben der Eintrittswahrscheinlichkeit des auslösenden Ereignisses (Handlung bzw. Umstand) ist die Eintrittswahrscheinlichkeit des Schadens selbst – gemessen als wahrscheinliche Schwere des resultierenden Schadens – zu beurteilen. Wesentliche Faktoren für die Bestimmung einer möglichen Schwere sind:

- *Die Verarbeitung besonderer Kategorien personenbezogener Daten.*
  Allerdings kann dies nicht bedeuten, dass automatisch ein schwerer Schaden bei der Verarbeitung solcher Daten vorliegen wird, sondern nur, dass hier genau zu bewerten ist, welche Art von „Schindluder“ mit solchen Daten getrieben werden kann.

- *Die Verarbeitung von besonders schützenswerten Kinder- und Beschäftigtendaten.*
  Hier muss anhand der Datenkategorien weiter beurteilt werden, ob dies wirklich ein (automatisch) „risikoerhöhendes“ Szenario ist. Geht es etwa (nur) um unternehmensbezogene Kontaktdaten eines Beschäftigten, die vielleicht sogar mit dessen Einverständnis auf der Unternehmens-Webseite veröffentlicht wurden, oder um die Notfall-Kontaktadresse des Kindes eines Beschäftigten (s. im Ausgangsfall betreffend die Huber AG), ist das Risiko ganz anders zu beurteilen als bei Daten über psychische Krankheiten von Kindern.

- *Die Verarbeitung nicht veränderbarer und eindeutig identifizierbarer Daten (Klarnamenverarbeitung).*
  Das Kurzpapier Nr. 18 der DSK nennt hier etwa *„eindeutige Personenkennzahlen im Vergleich zu pseudonymisierten Daten“*, obwohl gerade eine Personenkennziffer ein Pseudonym darstellt (s. dazu auch oben Fall 32). Trotz dieser Unklarheit ist aber im Grundsatz davon auszugehen, dass ein Schaden bei Kenntnis der „Klarnamenbeziehung“ erheblicher sein kann als nur bei Kenntnis eines Pseudonyms, da in diesem Fall der Täter zusätzlich auch an die Zuordnungsinformation (zwischen pseudonymen Daten einschließlich einer „Personenkennziffer“ und dem Klarnamen) gelangen muss. Dies kann aber nicht bedeuten, dass das „Abhandenkommen“ eines jeden Klarnamens – eine Vielzahl IT-gestützter Datenverarbeitungsvorgänge arbeitet mit Klarnamen (man denke nur an die Angabe des „Bearbeiters“ auf Angeboten, Auftragsbestätigungen, Rechnungen, Lieferscheinen oder an die Angabe des Klarnamens als

Alias-Namen im Rahmen einer E-Mail-Adresse) – sofort zu einem schwerwiegenden Schaden führt.

- *Automatisierte Verarbeitungen, die eine systematische und umfassende Bewertung persönlicher Aspekte (einschließlich Profiling) beinhalten und auf deren Grundlage dann Entscheidungen mit erheblichen Rechtswirkungen für betroffene Personen getroffen werden.*
  Dieses Kriterium wurde Art. 35 Abs. 3 lit. a DSGVO entnommen und impliziert dort eine hohe Schadensgeneigtheit. Die *„erheblichen Rechtswirkungen für betroffene Personen"* sind eine Umschreibung eines hohen Schadens, der im Umkehrschluss auch ein hohes Risiko (und damit die Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung) bedeutet.

- *Vollständige oder überwiegende Irreversibilität des Schadens (Irreversibilität).*
  Dies dürfte in erster Linie bei Veröffentlichungen von Daten bzw. Rufschädigung der Fall sein. Aber auch die Neutralisierung eines Identitätsmissbrauchs kann eine sehr lange Zeit in Anspruch nehmen. Daher darf daraus nicht im Umkehrschluss gefolgert werden, dass reversible Schäden grundsätzlich „unerheblich" wären. Die Reversibilität kann nur ein Indiz für das Vorliegen eines niedrigen Schadenspotenzials sein.

- *Der Betroffene hat nur wenige oder beschränkte Möglichkeiten, die Verarbeitung selbst zu prüfen oder gerichtlich prüfen zu lassen oder sich dieser Verarbeitung zu entziehen, etwa, weil er von der Verarbeitung gar keine Kenntnis hat (Intransparenz).*
  Eine derart intransparente Verarbeitung würde aber auch immer bedeuten, dass schon ein Datenschutzverstoß – zumindest in Form unterlassener Pflichtinformationen – bei der Erhebung der Daten vorlag. Eine weitere relevante Fallgruppe könnte hier die (Schadenswahrscheinlichkeit aufgrund der) Übermittlung in Drittländer sein, insbesondere bei Verstoß gegen die dem außereuropäischen Dritten auferlegten Pflichten (Standardklauseln der EU-Kommission, Privacy Shield etc.).

- *Die Verarbeitung ermöglicht eine systematische Überwachung.*
  Dieser Faktor ist Art. 35 Abs. 3 lit. c DSGVO entnommen (dort aber auf öffentliche Bereiche eingeengt) und dürfte in vielen Fällen bereits zum Vorliegen eines hohen Risikos und damit zur Erforderlichkeit einer Datenschutz-Folgenabschätzung führen.

- *Die Reichweite der Verarbeitung, namentlich die Anzahl der betroffenen Personen, die Anzahl der Datensätze, die Anzahl der Merkmale in einem Datensatz sowie die*

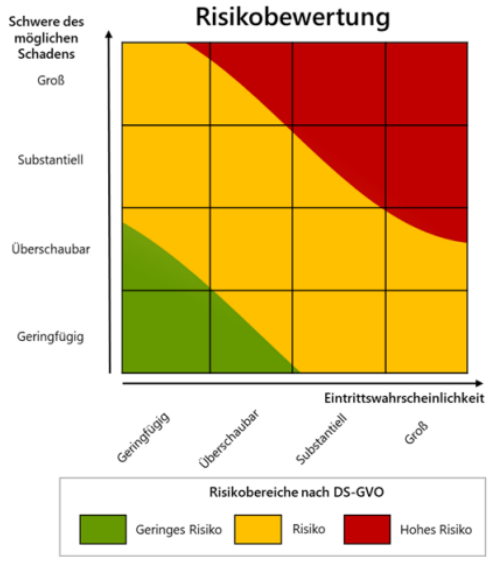
geographische Abdeckung, die mit den verarbeiteten Daten erreicht wird (Verarbeitungsreichweite).
Auch dies überschneidet sich mit den Kriterien im Rahmen der Schwellwert-Analyse.

Man wird hier insgesamt bemerken, dass solche Kriterien nur sehr eingeschränkt zur Bemessung eines hypothetischen Schadens taugen. Sie betreffen tendenziell eher – wieder einmal – die Intensität der Verarbeitungshandlungen selbst und nicht so sehr die Frage, ob ein Schaden, wenn er eintritt, hoch ist. Daher erscheinen die Kriterien (mit Ausnahmen) eher willkürlich und nicht „zielgerecht". Ohnehin kann im Bereich immaterieller Schäden, d. h. ohne Rückgriff auf Geldbeträge, eine Schadenshöhe schwer beziffert werden. Im Bereich der Schmerzensgeldbemessung bei Körperverletzungen mussten Gerichte auch im Laufe vieler Jahre eine Ansicht dazu entwickeln, ob eine Arm- oder Beinamputation für den Betroffenen „schädlicher" ist (nicht im Sinne von Behandlungskosten, sondern im Sinne des Verlusts als solchem). Die ersten (deutschen) Urteile in Sachen „Datenschutzschadenbemessung" (s. etwa oben Fall 9) lassen zumindest bislang eine eher skeptische Grundhaltung der Richter erkennen. So wurde in mehreren Gerichtsurteilen festgehalten, dass ein geldmäßiger Ersatz immaterieller Schäden eine gewisse Erheblichkeit der Datenschutzverletzung voraussetzt, und im konkreten Fall eine solche Erheblichkeit stets verneint. Mit den angedrohten Bußgeldern sind solche Beträge jedenfalls bislang nicht zu vergleichen.

Die verschiedenen Ursachen, die zuvor auf ihre Eintrittswahrscheinlichkeit hin untersucht wurden, spielen bei der Ermittlung der voraussichtlichen Schwere eines Schadens keine wesentliche Rolle. Hier ist nur zu untersuchen, welches Szenario zu welcher Schadenshöhe beim Betroffenen führen kann, gleich, wodurch es letztlich ausgelöst wurde. Dabei dürfte auch mit einzubeziehen sein, inwieweit in der Vergangenheit Vorfälle der untersuchten Art beobachtet wurden, denn aufgrund früherer Vorfälle könnte eine Eintrittswahrscheinlichkeit bzw. Schwere eines Schadens höher anzusetzen sein.

- Die Matrix

Nach der im Kurzpapier 18 der DSK skizzierten Methodik hat auf dieser Basis anhand einer Risikomatrix eine Risikobewertung des mit dem Verarbeitungsvorgang einhergehenden Risikos zu erfolgen:



Auch nach dieser Methodik kann sich also – unabhängig von den etwas abweichenden, oben verwendeten Katalogen typisierter Kriterien im Rahmen der Schwellwert-Analyse für die Datenschutz-Folgenabschätzung – als Ergebnis der Risikobewertung noch ein „hohes Risiko“ ergeben, welches die Durchführung einer Datenschutz-Folgenabschätzung notwendig macht. Dies bedeutet wohl letztlich, dass eine Schwellwert-Analyse und, selbst wenn diese „unauffällig“ geblieben ist, eine „normale Risikobewertung“ notwendig sind, um ein „hohes Risiko“ überhaupt definitiv zu identifizieren.

Übrigens führt das Kurzpapier 18 der DSK ergänzend aus, dass es sich in den Grenzbereichen in der obigen Matrix nicht um die Anwendung eines eindeutigen Schemas handelt, sondern eine Einzelfallbetrachtung notwendig ist:

„Bei der Abschätzung des Risikos anhand der Matrix können Fälle eintreten, in denen der Eintritt des Schadens relativ wahrscheinlich ist oder der potentielle Schaden besonders schwer wiegen würde und somit Grenzbereiche zwischen den Risikobereichen betroffen sein können. Hier sind in den Feldern der Matrix zwei Farben eingetragen. Dies macht deutlich, dass in diesen Grenzfällen eine Einzelfallbetrachtung notwendig ist. Diese kann im Zweifel zu dem Schluss kommen, dass trotz des Ergebnisses der generischen Abschätzung anhand der Matrix, der Einzelfall als so schwerwiegend erscheint, dass dennoch ein hohes Risiko gegeben ist. Umgekehrt kann im Einzelfall z. B. auch ein geringfügiger möglicher Schaden, der eine überschaubare Eintrittswahrscheinlichkeit hat, ein geringes Risiko darstellen.“

Ganz unabhängig davon, ob und wie diese Vorgaben in der Praxis umgesetzt werden können, wurde allerdings oben bereits darauf hingewiesen, dass die bloße Erkenntnis, dass der Datenverarbeitungsprozess X mit einem „normalen Risiko" versehen ist, nicht viel bringt. So sollen nach den besagten Checklisten normale Risiken „mit den üblichen Basismaßnahmen bereits adäquat adressiert werden". Welche genau das aber sein sollen – es ist ja nicht einmal klar, ob es um analoge oder digitale Sachverhalte geht –, bleibt offen. Es gibt gerade keinen Standard-Katalog technischer und organisatorischer Maßnahmen, die bei einem „normalen Risiko" anzuwenden wären, abgesehen vielleicht vom IT-Grundschutzkatalog des BSI im digitalen Bereich. Womöglich kann ein solcher Standard-Katalog auch gar nicht existieren, weil die Realität zu vielfältig ist. Vielmehr müssen technische und organisatorische Maßnahmen zu einem großen Teil individuell anhand der konkreten Verarbeitungssituation an die individuell identifizierten Risiken angepasst werden. Dies zeigt aber, dass die „Holzschnittartigkeit" des oben skizzierten Vorgehens bei der Risikobewertung nur zu wenig handfesten Konsequenzen führt. Die Datenschutzbehörden planen dennoch, die von ihnen aufgelisteten – und durchaus umfangreichen – „generischen Maßnahmen" in Abschnitt D1 des Standard-Datenschutzmodells (im Prinzip Vorschläge zur Entwicklung spezifischer technischer und organisatorischer Maßnahmen) um einen „Referenzmaßnahmen-Katalog" zu ergänzen, der Vorgaben für Maßnahmen *„bei normalem Ausgangsrisiko bzw. bei normalem Schutzbedarf"* sowie zusätzlich für Maßnahmen bei hohem Verarbeitungsrisiko enthalten soll. Bis dahin sind im Rahmen des vom Standard-Datenschutzmodells vorgesehenen Datenschutzmanagement-Prozesses (Abschnitt D4.4) die individuell aufgrund der Risikostruktur gewählten Maßnahmen mit den generischen Maßnahmen „abzugleichen".

Der im Rahmen des Standard-Datenschutzmodells vorgeschlagene Datenschutzmanagement-Prozess geht im Rahmen der Spezifikation von Datenverarbeitungsvorgängen davon aus, dass (risikoabhängig) Maßnahmen im technischen und organisatorischen Bereich festgelegt werden (Soll-Maßnahmen). Konkreter könnte man für den IT-Bereich sagen, dass Funktionen (bzw. die Überführung von Input- zu Output-Zuständen) von Systemen und Programmen definiert werden (Soll-Funktionalitäten). So könnte die Huber AG für sich festlegen, dass Stammdaten von Beschäftigten zehn Jahr nach deren Ausscheiden gelöscht werden müssen. Nach der Implementation entsprechender Funktionen wird der Ist-Zustand erhoben, insbesondere durch Protokollierung des „Outputs" (bzw. durch eine Kontrolldokumentation). Im Rahmen der Überprüfung der Maßnahmen können sich sog. „funktionale Soll-Ist-Differenzen" ergeben. Die von der Huber AG parametrisierte Software könnte etwa nicht in der Lage sein, bestimmte, von der Huber AG im Wege von Sonderentwicklungen hinzugefügte Datenfelder (die über den Standard-Lieferumfang der von der Huber AG eingesetzten

Software hinausgehen) zu löschen. Diese Differenzen können, vereinfacht gesagt, noch akzeptabel sein, weil sie das Restrisiko nicht signifikant erhöhen, oder nicht mehr akzeptabel sein, sodass der Prozess noch einmal durchlaufen werden muss. Die Huber AG müsste also bewerten, ob die „stehengelassenen" Daten für sich alleine so „risikoarm" oder anonym sind, dass ihre Löschung – oder deren Kontrolle – nicht zwingend erforderlich ist. Dabei muss die Huber AG sicherstellen, dass sie sämtliche relevanten Funktionen tatsächlich spezifiziert und prüft und nicht einzelne Funktionen ungeprüft einsetzt (s. dazu unten Fall 40).

All das gibt natürlich nicht die DSGVO selbst vor; es ist eher anzunehmen, dass die Autoren der DSGVO nicht einmal wussten, dass es solche Prozesse, die später (zum Teil auch früher) so komplex von den deutschen Datenschutzbehörden als „eigener Vorschlag" zur Umsetzung eines hochabstrakten Gesetzestextes formuliert wurden, überhaupt gibt. Sonst hätte ja auch das Standard-Datenschutzmodell die DSGVO bilden können und man hätte sich das „Mapping" von mehrdeutigem Gesetzestext und der eigenen Nomenklatur der Datenschutzbehörden – den „Gewährleistungszielen" – sparen können. Vielleicht sollte sich in Zukunft – wie im Steuerrecht – die vollziehende Verwaltung das dann von ihr anzuwendende Datenschutzrecht selbst schreiben und nicht ideologische Parlamentarier, denen es vorrangig nicht um europäische mittelständische Unternehmen, sondern um „die großen internationalen Datenkraken" ging (die mit der DSGVO bislang nicht getroffen wurden).

➢ Was sagt uns das?

Wer bis hierher gelesen hat, wird nun sicherlich für jeden End-to-End-Prozess der Datenverarbeitung in einem mittelständigen (oder gar größeren) Unternehmen eine permanente Risikobewertung einfach umsetzen können. Dabei bleibt natürlich zu hoffen, dass dieses pseudomathematische Risiko-Evaluierungsmodell nicht am Ende noch in Richtung Notwendigkeit einer Datenschutz-Folgenabschätzung führt. Oder anders ausgedrückt: Wenn man den hier wiedergegebenen (und kommentierten) Maßstab anwendet, wird jeder aufmerksame Betrachter ein Haar in der Suppe – sprich: im Ergebnis der Risikobewertung – finden können. Denn jeden unbestimmten (Rechts-) Begriff im Rahmen dieses Maßstabs kann man auch anders auslegen.

Was bleibt? Der Zweck von Risikobewertungen ist in erster Linie, demonstrieren zu können, dass sich ein Verantwortlicher (vermeintlich) systematisch Gedanken über seine Verarbeitungshandlungen gemacht hat. Ob er dabei zu den „richtigen" Schlussfolgerungen gekommen ist, ist letztlich gar nicht so wichtig, denn alles kann man „so oder so" sehen.

Entscheidend ist eher die richtige Rückkopplung an die technisch-organisatorischen Maßnahmen: Die szenario-spezifischen Risiken müssen durch adäquate (szenario-spezifische oder allgemeine) Maßnahmen der Datensicherheit soweit abgeschirmt werden, bis sie ein Maß erreichen, das vom Kurzpapier 18 der DSK als „Restrisiko" bezeichnet wird. Welches Restrisiko akzeptabel ist, wird nicht definiert. Ausschlaggebend dürfte die Verhältnismäßigkeit zwischen Maßnahmen (d. h. insbesondere dem für die Implementierung notwendigen Aufwand) und der dadurch (noch) erreichten Risikoeindämmung sein (Art. 24, 25, 32 DSGVO). Abschnitt D4.3 des Standard-Datenschutzmodell führt aus, risikonotwendig (und daher zu ergreifen) seien die Maßnahmen, die *„mit einem Aufwand ergriffen werden können, der in angemessenem Verhältnis zum Zweck der Verarbeitung besteht"*. Interessant ist dabei, aber das nur am Rande, dass auf den „Zweck", aber nicht auf das „Risiko" der Verarbeitung abgestellt wird. Dieses Verhältnis muss im Grundsatz spezifisch für den jeweiligen unternehmensinternen „end to end"-Prozess sowie im Hinblick auf die konkret betroffenen Datenkategorien bewertet und seine Angemessenheit „abgesegnet" werden. Letztlich muss das Restrisiko, wenn es nach dieser Verhältnismäßigkeitsformel nicht weitergehend abgeschirmt werden muss, dem Verantwortlichen auch „akzeptabel" erscheinen dürfen, denn ein Null-Prozent-Risiko kann nur durch Aufgabe der entsprechenden Verarbeitungshandlung erreicht werden. Was das alles im Detail heißt, weiß niemand. Nur eines ist sicher: Wenn am Ende etwas schief geht, wird es entweder an einer falschen Risikobewertung oder an „risikoinadäquaten" Maßnahmen liegen (denn „nachher ist man immer schlauer"). Und wenn nichts schief geht, wird schon alles richtig gewesen sein.

Fall 38:
Ein Protokoll wär‘ toll

Praktischer Fall: Die Huber AG verwendet eine ERP-Software, die sämtliche Veränderungen, die an den dort gespeicherten Daten – ob personenbezogen oder nicht – vorgenommen werden, protokolliert. Im Grunde lautet der Datensatz jeweils: „Datum X wurde in Datum Y geändert durch Z am [Datum, Uhrzeit]“. Für die Huber AG stellt sich die Frage, ob diese Protokolle datenschutzrechtlich vereinfacht gesprochen „zu viel“ oder sogar noch „zu wenig“ sind. Leider lässt sich die Protokollfunktion in der ERP-Software nicht abschalten oder sonst verändern. Auch können in der Software keine automatischen Löschregeln bzw. Löschfristen für derartige Protokolldatensätze festgelegt werden. Allenfalls ließen sich Protokolldatensätze manuell früher oder später (vollständig) löschen. Ein Überschreiben solcher Datensätze mit „Leerdaten“ würde nur seinerseits neue Datensätze über die Veränderung der Protokolldatensätze produzieren.

Protokolldaten werden in der Unternehmenspraxis in erheblichem Umfang generiert. Viele Applikationen erheben ständig Daten darüber, welche Benutzer (bzw. Benutzerkonten) Daten eingeben, verändern, abfragen und löschen. Dabei geht es nicht darum, dass diese Daten – als „Telemetrie-Daten“ – vom Hersteller der Software „abgezogen“ werden, sondern die generierten Daten werden regulär in der Datenbank gespeichert.

➢ Warum sind Protokolldaten gefährlich?

Im Fall 4 oben wurden Protokolldaten aus der Sicht von Auskunftsansprüchen beleuchtet. Aus derartigen Daten lassen sich allerdings – unabhängig von ihrem primären Zweck, unternehmensinterne Vorgänge nachzuvollziehen – verschiedenste Schlüsse über Beschäftigte ziehen. Daher geht es nicht nur im die „Beauskunftung“, sondern auch um die Frage, ob und in welchem Umfang es solche Daten geben darf bzw. muss. Insbesondere eine Profilbildung kann mit derartigen Daten betrieben werden: Arbeitszeiten, Abwesenheiten, Qualität und Geschwindigkeit von Eingaben etc. können aggregiert und in Beziehung zueinander gesetzt werden. Die Protokollierung von Nutzerdaten ist Gegenstand des Bausteins 43 des Standard-Datenschutzmodells, allerdings nicht so sehr hinsichtlich der „Gefährlichkeit“ bzw. „Ausnutzbarkeit“ solcher Daten (und daher ihrer möglichst sparsamen Erhebung und schnellen Löschung), sondern vor dem Hintergrund der datenschutzrechtlichen Rechenschaftspflicht. Diese Zweckrichtung fassen folgende einleitenden Ausführungen des Bausteins 43 (der die „Orientierungshilfe Protokollierung“ von 2009 ablöst) zusammen:

„Die Protokollierung dient der Prüfbarkeit einer Verarbeitung, die in der Vergangenheit stattfand. Zusammen mit der Spezifikation und Dokumentation ist sie eine wesentliche Voraussetzung, um eine Verarbeitung datenschutzrechtlich beurteilen zu können. Prüfbarkeit bedeutet, dass Ist- und Soll-Werte aller relevanten Verarbeitungseigenschaften ermittelt und verglichen werden und somit Prüfergebnisse erzeugt werden können, mit denen fachliche, organisatorische, technische und administrative Aktivitäten und Entscheidungen, die in der Vergangenheit im Rahmen einer Verarbeitung stattfanden, überprüfbar sind. Die Prüfbarkeit ist somit eine Voraussetzung für den Nachweis einer wirksamen Umsetzung der gesetzlichen Datenschutzanforderungen und deren Beurteilung. Eine Protokollierung muss die Frage beantworten können, welche Instanzen (Organisationseinheiten, Systeme oder handelnde Personen) welche Aktivitäten zu bestimmten Zeitpunkten ausgeführt und welche Instanz das Protokoll darüber geführt hat. Protokolle werden in aller Regel automatisiert erstellt („Logging"), können aber auch händisch geführt werden. Um einen lückenlosen Nachweis führen zu können, müssen Protokolldaten valide, reliabel, aktuell und vollständig sein. Zumindest bei hohem Schutzbedarf ist eine gesicherte Revisionsfestigkeit von Protokollen begründet."

Protokolldaten haben daher datenschutzrechtlich zwei Gesichter: Ihre Erstellung und Analyse ist eine technisch-organisatorische Maßnahme zur Absicherung der durch sie protokollierten (überwachten) Daten, und sie stellen ihrerseits personenbezogene Daten dar. Auf den ersten Aspekt ist am Ende dieses Falles noch zurückzukommen. Die (datenschutzrechtliche) Verarbeitung solcher Daten dürfte bei der Protokollierung von Eingaben in Fachapplikationen (im Rahmen von Geschäftsprozessen) *„für Zwecke des Beschäftigungsverhältnisses"* im Sinne des § 26 BDSG erfolgen, der eine Ausprägung der datenschutzrechtlichen Legitimationsgrundlage „Vertrag" (Art. 6 Abs. 1 S. 1 lit. b DGSVO) darstellt (s. oben Fall 4). Diese Zwecke sind, konkreter formuliert, die betrieblichen Belange des Verantwortlichen, die vom Mitarbeiter gemäß seiner anstellungsvertraglichen Aufgabenstellung umzusetzen sind, einschließlich der Möglichkeit zur Kontrolle der Sachbearbeitung durch den Beschäftigten als solcher (fachliche Qualität, inhaltliche Datenrichtigkeit). Während des laufenden Beschäftigungsverhältnisses obliegt es in erster Linie dem Arbeitgeber, im Rahmen der anstellungsvertraglich vereinbarten Position des Mitarbeiters zu definieren, welche Bewegungsdaten im Einzelnen verarbeitet werden und für welche weiteren Mitarbeiter diese einsehbar sind. In diesem Zusammenhang weist auch das Standard-Datenschutzmodell im Baustein 43 darauf hin, dass Protokolldaten nur zu den Zwecken geprüft werden dürfen, die Anlass für ihre Speicherung waren (Zweckbindung und Berechtigungskonzept):

„Weisen Protokolldaten einen Personenbezug auf, dürfen sie nur zu ausgewiesenen Zwecken von speziell dazu Befugten ausgewertet werden. Für die Protokollierung der Tätigkeiten von Mitarbeiter/-innen, Administrationstätigkeiten sowie der Aktivitäten von IT-Systemen und an Schnittstellen gelten ebenfalls der datenschutzrechtliche Zweckbindungsgrundsatz und die Regelungen des Beschäftigtendatenschutzes. Protokolldaten dürfen daher nur zu den Zwecken geprüft werden, die Anlass für ihre Speicherung waren. Um festzustellen, ob die Zweckbindung eingehalten wird, müssen Protokolldaten unterschiedlicher Ebenen – Protokollierung auf der Ebene der Sachbearbeitung, der Fachprogramme, der IT-Infrastruktur, der Administration – miteinander in eine Beziehung gesetzt werden können, um die Rechtskonformität aller Aktivitäten auf den verschiedenen Ebenen, die sich letztlich zumeist aus den gesetzlichen Regelungen der Fachlichkeit herleiten, nachweisen zu können.“

Auch für die – wie bei allen personenbezogenen Daten erforderliche – Löschung von Protokolldatenbeständen soll nach dem Baustein 43 des Standard-Datenschutzmodells die aus der „Fachlichkeit“ abgeleitete Löschfrist maßgeblich sein. Was dies im Detail bedeutet, ist unklar, da die zugrundeliegenden (z. B. vom Mitarbeiter geänderten) Daten nicht personenbezogen sein müssen und dann auch keine Löschfristen einschlägig sind.

- Viel hilft viel

Die von Baustein 43 hervorgehobene Vorgabe der DSGVO, die Rechtmäßigkeit sämtlicher Verarbeitungen personenbezogener Daten nachweisen zu können (Rechenschaftspflicht, *„accountability“*), würde nun an sich eine Protokollierung sämtlicher datenschutzbezogener Einzelvorgänge mit sämtlichen Details erfordern: Je mehr, desto besser. Dies kann sich allerdings nur auf den Zugriff auf solche (mit den Protokolldaten überwachten) Daten im ERP-System beziehen, die ihrerseits personenbezogen sind. In diesem Kontext dienen Protokolltätigkeiten einer verwendeten Applikation aus datenschutzrechtlicher Perspektive dem Zweck, einen lückenlosen Nachweis führen zu können, welche Entität (Person, System) welche datenschutzrelevanten Aktivitäten zu welchem Zeitpunkt ausgeführt und welche Entität darüber Protokoll geführt hat. Die Protokollierung von Verarbeitungsvorgängen mit nicht personenbezogenen Daten kann diesem Zweck von vornherein nicht dienen.

In Sinne der datenschutzrechtlichen Rechenschaftspflicht fordert Baustein 43 des Standard-Datenschutzmodells zusätzlich zur Protokollierung der Nutzeraktivitäten einer Fachapplikation auch die Protokollierung von Systemaktivitäten, Administrationstätigkeiten und Schnittstellenaktivitäten. Ziel ist es, anhand der Protokolle die Einhaltung datenschutzrechtlicher Vorgaben oder bei der Aufklärung von Datenschutzverstößen deren Ursache und Ausmaß

nachweisen zu können, weshalb Protokolldaten valide, unveränderbar, aktuell und vollständig sein müssen. Gerade die Nutzung administrativer Rechte muss zu einem Eintrag im Protokoll führen, auch zum Schutz des Administrators vor unberechtigten Vorwürfen.

Ähnlich umfangreich wird die Protokollierung des Zugriffs (zumindest) auf sensible Daten auch in einem Fallbeispiel des Europäischen Datenschutzausschusses in seinen Empfehlungen vom November 2019 zum Thema *„privacy by design / by default"* beschrieben:

„A controller wants to extract personal data from a medical database to a server in the company. The company has assessed the risk for routing the extracts to a server that is accessible to all of the company's employees as likely to be high for data subjects' rights and freedoms. There is only one department in the company who needs to process these patient data. The extracts will also have a high value to the company. To regulate access and mitigate possible damage from malware, the company decides to segregate the network, and establish access controls to the server and the directory. In addition, they put up security monitoring and an intrusion detection and prevention system. The controller activates access control on the server and isolates it from routine use. An automated auditing system is put in place to monitor access and changes. Reporting and automated alerts are generated from this when certain events related to usage are configured. This security measure will ensure that all users have access on a need to know basis and with the appropriate access level."

➢ Datenminimierung als Gegengewicht

Derart umfangreiche Protokolldaten führen – um der Rechenschafts- und damit Protokollpflicht willen – ihrerseits zu einer großen Menge personenbezogener Daten. Dabei gerät der Grundsatz der Datenminimierung in den Fokus, der natürlich auch eine „Protokolldatensammelwut" begrenzt. Zwei Gesichtspunkte können zur Steuerung des Datenaufkommens eine entscheidende Rolle spielen:

- Zum einen sollte bei der Protokollierung, wenn diese personenbezogene Daten beinhaltet, auf die zugehörigen Inhaltsdaten verzichtet werden, sodass es sich um reine Metadaten handelt. Denn mit der Protokollierung „X in Y geändert durch Z am [Datum, Uhrzeit]" werden die personenbezogenen Daten X auch noch im Protokolldatensatz (vervielfältigt und) „perpetuiert": Eine Löschung von X muss daher auch Teile des Protokolldatensatzes löschen. Auch der Zugriff auf die Protokolldaten muss den datenschutzrechtlichen Grundsätzen, etwa einem Berechtigungskonzept, unterliegen. Die Datenschutzbehörden fordern teils auch die Verschlüsselung und Signierung der Protokolldaten nach dem Stand der Technik.

- Zum anderen können bei der Sachbearbeitung – je nach Risikoeinschätzung – in Bezug auf Daten das Lesen (Dateneinsicht), die Eingabe, die Änderung, das Sperren, das manuelle Löschen, die Übermittlung sowie die Nutzung automatisierter Abrufverfahren relevant sein. Die Frage, bei welcher Risikointensität welche Protokollierungs-Intensität erforderlich ist, wird weder im Standard-Datenschutzmodell noch in anderen Veröffentlichungen der Datenschutzbehörden beantwortet. Gerade eine – sehr datenintensive – Protokollierung von Lesezugriffen wird im Grundsatz nur bei sehr sensiblen Daten notwendig sein.

Zum letztgenannten Punkt (Protokollierung von Lesezugriffen) hatte die „Orientierungshilfe Protokollierung" der Datenschutzbehörden aus 2009 noch Folgendes bestimmt:

„Eine Protokollierung lesender Zugriffe ist ebenso aus Gründen der datenschutzrechtlichen Revisionssicherheit grundsätzlich erforderlich, insbesondere wenn ein Verfahrensschritt für den Nutzer direkt auf die Ermittlung personenbezogener Daten abzielt. Bei einem hinreichend fein differenzierten Zugriffsschutz kann der Umfang der Protokollierung reduziert werden."

So apodiktisch lässt sich eine solche „grundsätzliche Erforderlichkeit" dem Standard-Datenschutzmodell nicht (mehr) entnehmen. Wie der Umfang derartiger Protokolldaten durch einen *„hinreichend fein differenzierten Zugriffsschutz"* verringert werden kann, blieb ohnehin offen.

➢ Risikoerhöhung – und nochmal von vorn!

Aus Sicht des Standard-Datenschutzmodells (Abschnitt D3.4) stellt die Protokollierung eine potentiell risikoerhöhender technische Maßnahme dar, die ihrerseits neue technische und organisatorische Maßnahmen erforderlich machen kann:

„Zu beachten ist, dass neue Risiken durch ergriffene technische und organisatorische Maßnahmen entstehen können. Diese Risiken sind zu bewerten und angemessen zu reduzieren. Als Beispiel kann eine Vollprotokollierung von Mitarbeiter-Handlungen gefordert sein, die zugleich das Risiko birgt, dass durch Auswertungen dieses Protokolls eine unzulässige Leistungs- und Verhaltenskontrolle stattfindet. Wird in diesem Schritt eine Verarbeitung so verändert, dass die getroffenen Maßnahmen zu neuen Risiken, die höher sind als das Ausgangsrisiko, und somit zu einer Erhöhung des Schutzbedarfs führen, muss die Ausgestaltung der

Maßnahmen erneut evaluiert werden. Die oben genannten Strategien sind in einem iterativen Prozess so lange anzuwenden, bis die Ausgestaltung der Maßnahmen ein angemessenes Schutzniveau gewährleistet.“

Das klingt nach einem nicht unerheblichen Umsetzungsaufwand.

Nur der Vollständigkeit halber ist darauf hinzuweisen, dass auch Protokolldaten Teil eines dokumentierten Löschkonzepts sein müssen. In Bezug auf die Vorgaben zum Löschen selbst (s. oben Fall 28) ergeben sich keine Besonderheiten. Da meist keine spezifisch auf Protokolldaten anwendbaren Aufbewahrungspflichten bestehen, ist im Regelfall die Erfüllung des Protokollierungszwecks maßgeblich für die Löschpflicht (Art. 17 Abs. 1 lit. a) DSGVO). Die Datenschutzbehörden haben in der Vergangenheit – aus im Einzelnen ungeklärten Gründen – Speicherfristen von einem bis mehreren Jahren für erforderlich gehalten. Längere Speicherfristen können insbesondere dann angezeigt sein, wenn ein Protokoll der Dokumentation eines unternehmensinternen Verfahrens dient (Kontrolldokumentation über die tatsächliche Anwendung des Prozesses) und eine Dokumentationspflicht für eine längere Dauer besteht, etwa bei der Protokollierung von Berechtigungen (Erteilung und Entzug von Zugriffsrechten, Anlegen und Löschen von Benutzerkennungen) oder in Industriebereichen mit spezifischen Aufzeichnungspflichten (Arzneimittelherstellung etc.).

- Geht’s denn überhaupt?

Selbst wenn die Huber AG nun im Rahmen ihrer (Risiko-) Analysen und Spezifizierung („Lastenheft“) ihrer ERP-Software verschiedene Anforderungen an die Beschaffenheit, den Umfang und die Löschung von Protokolldaten definiert hat, wird sich in der Praxis herausstellen, dass die konkret eingesetzte Software dies nicht leistet. Für diesen Fall sieht der Baustein 43 vor:

„Bei bestehenden Systemen müssen sämtliche Protokolldaten inventarisiert werden inklusive den Nachweis darüber, dass diese Protokollinhalte gesichtet und deren Relevanz für den Datenschutz beurteilt wurde.

Bereits in der Spezifikationsphase muss definiert werden, für welche Fragen und Prüfungen welche Protokolldaten erforderlich sind. Insbesondere wenn marktgängige Standard-Programme eingesetzt werden sollen wird es notwendig sein, noch vor der Inbetriebnahme zu prüfen, welche Protokolldaten standardmäßig erzeugt werden und ggfs. datenschutzrechtlich erforderliche Änderungen beim Hersteller zu verlangen.“

Die hier unterstellte „Nachfragemacht“ gegenüber dem Software-Hersteller – also das, was sich der DSGVO-Gesetzgeber als Folge der „*privacy by design*“-Verpflichtung der Verantwortlichen erhofft hat – bleibt in der Praxis aber selbst bei kleineren Anbietern häufig eine Illusion. Eine datenschutzrechtliche Neuorientierung einer „gewachsenen“ Software erfordert meist Veränderungen des grundlegenden Programm-Designs, d. h. der Daten(bank)struktur, und geht nicht mit „attraktiven neuen Funktionen“ einher, mit denen jede neue Programmversion idealerweise am Markt auftrumpfen sollte.

- Was macht man mit all den Daten?

Unabhängig davon sieht Baustein 43 für die Verarbeitung der so gewonnenen „rohen“ Protokolldaten eine – im besten Fall skriptgesteuerte und in jedem Fall dokumentierte – Filterung, Normalisierung, Aggregation, Kategorisierung und Priorisierung vor. Das Ergebnis soll insbesondere zur Generierung relevanter Aussagen über Auffälligkeiten (im datenschutzrechtlichen Sinne) führen, die dann auch zum Auslösen von (Abhilfe-) Aktionen führen können.

Dass dies keine graue Theorie ist, zeigt ein Bußgeldbescheid der polnischen Datenschutzaufsicht in einer Größenordnung von 600.000 Euro vom September 2019, der zwar keine Protokollierung interner Vorgänge (wie im Ausgangsfall der ERP-Software der Huber AG) betrifft, aber dennoch die Notwendigkeit der Anfertigung und (laufende) Analyse von Protokolldaten – hier: des externen Netzwerkverkehrs – aufzeigt. Für einen Identitätsmissbrauch geeignete Daten von 2,2 Millionen Betroffenen gerieten durch unzureichende Vorsichtsmaßnahmen in falsche Hände. Man kann dies allgemein als unzureichende technische und organisatorische Maßnahmen bezeichnen oder konkreter im Sinne von „*ineffective monitoring of potential risks*“:

„*There was a lack of appropriate response procedures to deal with the emergence of unusual network traffic.*“

Auffälliger Netzwerkverkehr, über den massenhaft personenbezogene Daten „abgezogen“ werden, auffällige Veränderungen von Bankdaten von Geschäftspartnern in einem ERP-System: Die richtigen Protokolldaten weisen den Weg zum Datenschutzverstoß. Der Sinn entsprechender Überlegungen sollte jedem Unternehmen klar sein. Aber welchen (signifikanten) Aufwand die Huber AG nun konkret erbringen muss, um eine Vielzahl von Szenarien nachvollziehbar zu evaluieren und – unter anderem – durch entsprechende und gut dokumentierte Protokollmechanismen „aufdeckbar“ zu machen, bleibt offen.

Fall 39: Der verflixte Fragebogen

Praktischer Fall: Die Anton Müller gGmbH erbringt gegenüber kleineren Institutionen und Organisationen Hilfestellungen im sozialen Bereich. Sie möchte ihre „Kunden" zur Zufriedenheit mit ihren Leistungen befragen und lädt daher die Mitarbeiter ihrer „Kunden" ein, einen Online-Fragebogen auszufüllen. Dieser Fragebogen ist in einen Teil I und einen Teil II gegliedert. Im ersten Teil wird der Betroffene gefragt, zu welcher Institution bzw. Organisation er zählt, wie lange er dort bereits tätig ist, zu welcher Hierarchieebene er zählt etc. Aus der Beantwortung dieser Fragen kann in einigen Fällen durchaus der Betroffene identifiziert werden. Der zweite Teil enthält Fragen, die sich auf die Sichtweise der Organisation bzw. Institution selbst als „Kunde" der Anton Müller gGmbH beziehen. Die Anton Müller gGmbH fragt sich, welchen datenschutzrechtlichen Aufwand sie im Umfeld der Online-Umfrage betreiben muss.

Auch dieser Fall spielt – wie schon oben Fall 32 – an der „Grenzlinie" zwischen anonymen und nicht-anonymen Daten. Geht man davon aus, dass die Anton Müller gGmbH von vornherein über persönliche E-Mail-Adressen der befragten (natürlichen) Personen verfügt und diese mit deren Hilfe und einem personalisierten Link (der den Befragten identifiziert) zum Ausfüllen „einlädt", ist der Fall schnell zu Ende, denn dann handelt es sich von vornherein um personenbezogene Daten und die Identität des jeweiligen Betroffenen ist bekannt. Fehlt ein solcher personalisierter Link und erfolgt das Besuchen der Webseite zum Ausfüllen des Fragebogens „anonym", befinden wir uns ebenso in einem Graubereich wie wenn lediglich dem „Kunden" selbst (Organisation / Institution) ein Link auf die Webseite mit dem Fragebogen (an ein Funktionspostfach) geschickt wird und der Link dann intern beim Kunden weitergeben kann.

➢ Warum Graubereich?

Wenn einzelne „Kunden" über eine derart kleine Belegschaft verfügen, dass die Fragen des Teils I die Person des Ausfüllenden identifizierbar machen, würde keine „echte" Anonymität mehr vorliegen. Wenn nach Beantwortung des Teils I feststeht, dass der Betroffene beim Kunden XY – der über 14 Mitarbeiter verfügt – tätig ist, dort seit über fünf Jahren beschäftigt ist – was die Auswahl auf zwei Mitarbeiter verengt, weil der Kunde erst seit sechs Jahren existiert – und die ausfüllende Person zur „Geschäftsführungsebene" zählt, kann dies – wenn nur noch ein Geschäftsführer aus der damaligen Zeit übrig geblieben ist – die ausfüllende Person identifizierbar machen. Mit ein wenig Recherche ist die Person dann womöglich schnell tatsächlich identifiziert. Die Antworten des Teils II können dann dieser Person zugeordnet werden und sind personenbezogene Daten dieser Person. Eine „echte Anonymität"

wird nach einer Einschätzung des Landesdatenschutzbeauftragten von Baden-Württemberg in dessen Ratgeber Beschäftigtendatenschutz vom März 2019 erst dann unterstellt, wenn mindestens sieben Personen sämtliche zur Verfügung stehenden Identifikationsmerkmale erfüllen und so eine genügend diffuse Gruppe bilden.

Dieser Graubereich kann prinzipiell dadurch verlassen werden, dass der Teil I einfach weggelassen wird und die Einladung und Teilnahme anonym erfolgt. Ohnehin stellt sich die Frage, ob nicht aufgrund der „*privacy by default*"-Vorgabe des Art. 25 Abs. 2 DSGVO die Antworten des Teils I standardmäßig „ausgegraut" sein müssten oder ob der Zweck der Befragung so weit definiert werden kann, dass die Antworten auf diese Fragen für die Befragung tatsächlich „erforderlich" sind. Ohne die Angaben zur Person (Teil I) müssten es schon die „sachlichen" Antworten im Teil II selbst sein – je nachdem, was im Fragebogen abgefragt bzw. eingegeben werden kann –, welche die Person identifizierbar machen. Dies wird im Regelfall ungleich schwieriger sein.

- Einwilligung und Widerrufsmöglichkeit

Gehen wir nun davon aus, dass als Legitimationsgrundlage für die Verarbeitung der Antworten im Fragebogen nur eine Einwilligung in Betracht kommt (s. oben Fall 17), so muss die Erteilung der Einwilligung später nachweisbar sein. Natürlich wird in derartigen Fallgestaltungen auch eine Interessenabwägung als taugliche Legitimationsgrundlage vertreten, was richtig oder auch falsch sein kann. Neben den Pflichtinformationen muss dem Betroffenen also die Widerruflichkeit seiner Einwilligung mitgeteilt werden (s. oben Fall 8). Die Durchführung dieser Aufklärungen des Betroffenen kann wohl durch entsprechende Prozesse, die vom Betroffenen durchlaufen werden müssen, nachgewiesen werden (s. oben Fall 1). Es ist demnach in diese Stadium (wahrscheinlich) keine Protokollierung eines individuellen „Zugangsnachweises" (Quittierung des Erhalts der Pflichtinformationen) erforderlich.

Die Frage ist aber nun, wie der Betroffene den Widerruf seiner Einwilligung geltend machen kann. Wenn er die Anton Müller gGmbH anschreibt und sinngemäß erklärt, er habe „neulich" einen Fragebogen ausgefüllt und wolle nun seine Einwilligung widerrufen (oder einer Interessenabwägung widersprechen), kann diese Eingabe in dieser Form keinem konkreten Datensatz zugeordnet werden. Die Anton Müller gGmbH müsste also mehr Daten erheben, um später das Widerrufsrecht überhaupt umsetzen zu können.

Neben der Möglichkeit zum Widerruf der Einwilligung müssen natürlich auch die anderen Betroffenenrechte erfüllt werden, d. h. Auskunftsrecht, Berichtigungsrecht, Löschrecht etc. Am besten wäre es natürlich – so würden die Datenschutzbehörden argumentieren –, wenn

der Betroffene auf der Online-Plattform selbst die Möglichkeit hätte, über einen persönlichen Zugang (Benutzername – der natürlich auch pseudonym sein kann wie „blabla123“ – und Passwort) seine Daten einzusehen, zu löschen und ggf. richtigzustellen (oder sogar zu exportieren).

➢ Keine Datenerhebung nur zu „DSGVO-internen“ Zwecken

Gesetzt den Fall, diese Möglichkeit ist nicht gegeben – was seinerseits zu einem Problem mit dem „*privacy by design*“-Grundsatz führen kann (s. unten Fall 40) –, kommt es auf eine Vorschrift an, die es in sich hat: Art. 11 DSGVO. Nach dieser Regelung müssen, salopp gesagt, keine personenbezogenen Daten extra deswegen erhoben werden, nur damit die DSGVO, insbesondere die Betroffenenrechte, eingehalten werden kann. Dieses Prinzip kann aus dem Grundsatz der Datenminimierung hergeleitet werden.

Art. 11 Abs. 1 DSGVO gilt für den Fall, dass der Verantwortliche zwar über personenbezogene Daten verfügt, diese aber die betroffene Person nur „identifizierbar“ machen. Die Person ist nicht „identifiziert“, d. h. ihre Kontakt- bzw. Adressdaten fehlen und sie kann nicht angesprochen bzw. angeschrieben werden. Sie müsste „identifiziert“ werden, was zwar möglich wäre (sie ist ja „identifizierbar“), aber nur zur Erhebung weiterer Daten über die Person führen würde. Dies gilt insbesondere auch in dem Fall, in dem nur ein Pseudonym bekannt ist, unter dem die Person erreicht werden kann, etwa eine Telefonnummer, unter welcher der Verantwortliche theoretisch auch anrufen könnte, um zu versuchen, Namen und Anschrift zu ermitteln: In derartigen Fällen ist die weitere Datenerhebung nicht geboten.

Die fehlende Pflicht zur Identifizierung eines Betroffenen kann so weit führen, dass diesem auch keine Pflichtinformationen zur Verfügung gestellt werden müssen, selbst wenn die Identifizierung möglich und zumutbar wäre, weil dies weitere Datenerhebungen voraussetzen würde. In der Kommentarliteratur wird als Beispiel ein Geoinformationsdienst wie Google Streetview genannt, dessen Betreiber natürlich herausfinden könnte, wer die Eigentümer und Bewohne abgebildeter Häuser sind, um diese über die Verarbeitung von Hausansichten – soweit dies personenbezogene Daten sind – zu informieren. Dies gilt aber natürlich nicht in Fällen wie dem vorliegenden, in dem ein direkter Kontakt mit einem – mehr oder weniger anonymen – Betroffenen besteht.

➢ Identifikationsprobleme

Vor diesem Hintergrund stellen sich nun zwei Probleme. Einerseits soll eine nur identifizierbare, aber nicht identifizierte Person vom Betroffenen darüber informiert werden, dass dieser

„nicht in der Lage ist, die betroffene Person zu identifizieren“, sofern diese Unterrichtung möglich ist (Art. 11 Abs. 2 DSGVO). Das trifft aber eigentlich nicht den damit wohl „gemeinten“ Fall: Der Verantwortliche ist in der „gemeinten“ Fallgestaltung sehr wohl in der Lage, die betroffene Person zu identifizieren – wäre er es nicht, wäre nämlich die DSGVO gar nicht anwendbar –, nur ist dies nicht geboten, weil dadurch (noch) mehr Daten verarbeitet werden müssten. So muss also nur der zur Verfügung stehende „Kanal“ – sofern es diesen (in der Regel in Form eines Adress-Pseudonyms) gibt – genutzt werden, um dem Betroffenen mitzuteilen, dass man nicht weiß, wer er ist. Muss man also im obengenannten Beispiel der (einzig) vorliegenden Telefonnummer doch unter der Nummer anrufen und demjenigen, der abnimmt, diese Information kolportieren?

Das zweite Problem liegt darin, wie ein Betroffener, dessen Identität der Verantwortliche nicht kennt, dessen Daten aber vom Verantwortlichen verarbeitet werden, Betroffenenrechte geltend machen kann. Die DSGVO sieht vor, dass in derartigen Situationen keine Betroffenenrechte nach den Artikeln 15 bis 20 DSGVO bestehen, *„es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Artikeln niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen“* (Art. 11 Abs. 2 S. 2 DSGVO).

Dies führt zu zwei Folgeüberlegungen. Einerseits sind der Widerruf der Einwilligung (Art. 7 DSGVO) und der Widerspruch gegen eine Interessenabwägung (Art. 21 DSGVO) nicht ausgeschlossen, sondern nur die Rechte der Artikel 15 bis 20 DSGVO, d. h. selbst dann, wenn die betroffene Person keine zusätzlichen Informationen zur Identifizierung bereitstellt, müssen diese Rechte „ausübbar“ sein. Es stellt sich also die Frage, wie der Widerruf eines Betroffenen einem Datensatz zugeordnet werden kann, wenn der Betroffene keine weitere Informationen bereitstellt – was er in diesem Fall nicht muss.

Andererseits: Selbst wenn der Betroffene weitere Informationen bereitstellen muss, um seine Betroffenenrechte nach Art. 15 bis 20 DSGVO – also beispielsweise ein Auskunftsrecht – doch ausüben zu dürfen, ist offen, wie der Verantwortliche diese Daten verifizieren und damit die korrekte Zuordnung zum relevanten Datensatz herstellen kann. Im Ausgangsfall könnte etwa jemand, der über die Antworten zu Teil I des Fragebogens identifizierbar ist, ein Auskunftsrecht geltend machen. Dies setzt voraus, dass er mitteilt, bei welchem „Kunden“ der Anton Müller gGmbH er seit wann in welcher Position tätig ist und dies dem Verantwortlichen ggf. nachweist. Der Verantwortliche müsste nun seinerseits – wie auch immer – verifizieren, dass es niemand anderes gibt, auf den das entsprechende Muster der Antworten in Teil I zutrifft. Ansonsten würde dem Betroffenen der Datensatz eines anderen Betroffenen als Auskunft bzw. Kopie übermittelt – ein klassischer Datenschutzverstoß.

Ein in der Kommentarliteratur genannter Fall betrifft in diesem Zusammenhang die Erfassung von Kfz-Kennzeichen in einem Parkhaus. Die Erteilung der Pflichtinformationen ist durch einen entsprechenden Aushang an den jeweiligen, nur identifizierbaren Betroffenen möglich. Dem Parkhausbetreiber ist insbesondere nicht bekannt – und er muss das auch nicht ermitteln –, ob der Fahrer im Parkhaus gleichzeitig der Halter des Wagens mit dem Kennzeichen ist. Wenn nun ein Halter, der nicht der Fahrer war, einen Auskunftsanspruch gegenüber dem Parkhausbetreiber geltend macht, wie kann der Parkhausbetreiber dann verifizieren, dass er den „richtigen" Betroffenen vor sich hat? Die Literatur geht davon aus, dass dem Halter, der sein Kfz-Zeichen angibt – die Richtigkeit dieser Information könnte möglicherweise durch den Verantwortlichen verifiziert werden –, die Auskunft zu erteilen ist. Aber wenn der tatsächliche Fahrer auf keinen Fall wollte, dass der Halter erfährt, dass und wie lange er im Parkhaus war?

- Wie widerrufen?

Zurück zum Ausgangsfall: Kann ein Widerruf der Einwilligung einem bestimmten Betroffenen zugeordnet werden, wird sich die Frage stellen, wie sich dies auf die weitere Auswertung der Fragebögen auswirkt. Erfolgt der Widerruf zeitlich vor einer weiteren (statistischen) Verarbeitung, ist der Fragebogen zu löschen und darf nicht in das Gesamtergebnis eingehen. Möglicherweise ließe sich aber auch argumentieren, dass nur der betreffende Teil I des Fragebogens zu löschen ist, weil Teil II dadurch anonym wird. Und Anonymisieren soll ja gleichwertig mit Löschen sein, selbst wenn der Vorgang des Anonymisierens seinerseits eine Verarbeitungshandlung ist, die einer datenschutzrechtlichen Legitimation bedarf (s. oben Fall 32). Erfolgt der Widerruf nach bestimmten Auswertungshandlungen, bleibt die Rechtmäßigkeit dieser Auswertungen (auch betreffend Teil I) unberührt, sofern die Auswertung der Fragebögen zu einem so hohen Aggregationsgrad führt, dass diese keine personenbezogene Information mehr darstellt (d. h. die aggregierten Daten sind anonym). Der Fragebogen muss dann also nicht aus den statistischen Ergebnissen „herausgerechnet" werden.

Am Ende noch ein neuralgisches Thema sämtlicher Informationserhebungen in digitaler Form: Freitextfelder. Sieht der Fragebogen am Ende vor, dass der Betroffene einen Kommentar in einem Freitextfeld hinterlassen kann, so kann dieser natürlich mit personenbezogenen Daten – auch dritter Personen – befüllt werden. Ein Paradebeispiel wäre: „Insbesondere Klaus Ludwig von der Organisation ‚Blumenfreunde' hat auf mich einen sehr befremdlichen Eindruck gemacht, als er beim letzten Sommerfest nackt und besoffen um das Lagerfeuer getanzt ist". In diesem Fall braucht die Anton Müller gGmbH für die Erhebung dieser Daten eine (dokumentierte) datenschutzrechtliche Rechtsgrundlage und der hier genannte Klaus

Ludwig müsste über die Erhebung dieser Daten durch die Anton Müller gGmbH – an der er persönlich nicht mitgewirkt hat – spätestens innerhalb eines Monats mit entsprechenden Pflichtinformationen benachrichtigt werden (Art. 14 DSGVO).

Fall 40: Menschenfreundlich, datenschutzfreundlich?

Praktischer Fall: Die Huber AG ist ein Telekommunikationsunternehmen, dessen Kunden ihre Rufnummer bei einem Anbieterwechsel auf einen Dritten übertragen können (Rufnummernportierung). Daneben verfügt die Huber AG über eine „do not call"-Liste derjenigen Kunden, die nicht zu Marketingzwecken kontaktiert werden möchten. Aufgrund einer fehlerhaft implementierten Software wurden in vielen Fällen bei einem Wunsch nach Rufnummernportierung, der später vom Kunden widerrufen wurde (d. h. der Kunde wollte doch Kunde der Huber AG bleiben), der Eintrag des Kunden in der „do not call"-Liste zwar beim ursprünglichen Antrag auf Anbieterwechsel gelöscht (weil die Rufnummer dann generell aus der Kundenkartei entfernt wird), aber beim späteren Widerruf nicht wieder in die Liste aufgenommen. Als Folge hat die Huber AG die betroffenen Kunden wieder für Marketing-Aktionen kontaktiert.

Letztlich geht es hier „nur" um eine fehlerhaft implementierte Software. Der Fall geht auf einen Bußgeldbescheid der griechischen Datenschutzbehörde vom Oktober 2019 zurück. Die griechische Behörde sanktionierte nicht nur das „legitimationslose" Ansprechen von (doch beim Telekommunikationsanbieter verbliebenen) Kunden als solches – also den konkreten „Außenverstoß" –, sondern auch die fehlerhafte Software-Implementierung an sich unter dem Gesichtspunkt der „*privacy by design*"-Vorgabe (Art. 25 Abs. 1 DSGVO). Ebenso erging es demselben Telekommunikationsunternehmen mit ihrer „Abmelden"-Funktion für aktive Kunden: Wenn diese auf die „*unsubscribe*"-Schaltfläche drückten, passierte – zumindest seit 2013 – nichts. Etwa 8000 Kunden waren von diesem zweiten Software-Fehler betroffen.

Das dafür in Summe verhängte Bußgeld in Höhe von 400.000 Euro, das auch andere Normen, gegen die verstoßen worden war, umfasste, ist hier nicht so wichtig. Entscheidend ist, dass die (fahrlässig verursachte) Fehlfunktion einer Software sanktioniert wurde: Durch den Fehler war die Software zumindest insoweit nicht mehr „datenschutzfreundlich". Man kann daraus in erster Näherung den (trivialen) Schluss ziehen, dass wenn eine von einem Unternehmen eingesetzte Software einen Datenschutzverstoß verursacht, nicht nur der verursachte Datenschutzverstoß relevant ist, sondern auch die Fehlerhaftigkeit der Software als Fehlleistung des Verantwortlichen im Rahmen der Planung (Spezifikation).

Diese Anforderungen an die „Prozess-Design-Phase" betreffen nicht nur die Planung und Implementierung von Software, sondern jegliche technische und organisatorische Maßnahmen, mit denen die Einhaltung der datenschutzrechtlichen Anforderungen sichergestellt

werden soll (s. dazu auch oben Fall 37). Schließlich hätte im Ausgangsfall das Register auch manuell geführt werden können und es hätte nur an einer Prozessvorgabe fehlen müssen, bei Widerruf der Portierung die entsprechende Rufnummer wieder auf die „do not call"-Liste zu setzen. Die Austauschbarkeit von technischen Maßnahmen einerseits und organisatorischen Maßnahmen andererseits – und die prinzipiellen Vorzüge der technischen Maßnahme – zeigt ein Fallbeispiel in den Empfehlungen des Europäischen Datenschutzausschusses vom November 2019 zum Thema *„privacy by design / by default"* im Hinblick auf ein Löschkonzept:

„The controller collects personal data where the purpose of the processing is to administer a membership with the data subject, the personal data shall be deleted when the membership is terminated. The controller makes an internal procedure for data retention and deletion. According to this, employees must manually delete personal data after the retention period ends. The employee follows the procedure to regularly delete and correct data from any devices, from backups, logs, e-mails and other relevant storage media. To make deletion more effective, the controller instead implements an automatic system to delete data automatically and more regularly. The system is configured to follow the given procedure for data deletion which then occurs at a predefined regular interval to remove personal data from all of the company's storage media. The controller reviews and tests the retention policy regularly."

Dies macht deutlich, dass die frühzeitige Strukturierung unternehmensinterner Prozesse – oder eben der diese Prozesse automatisierenden Software – unter Datenschutzgesichtspunkten von großer Wichtigkeit ist. In diesem Rahmen muss, wie der Ausgangsfall zeigt, auch ein ausführliches Testen der Funktionen unter realen Bedingungen erfolgen. Ein zwischen 2013 und 2019 nicht funktionierender Software-Bestandteil wäre im Bereich einer unternehmenskritischen bzw. direkt mit dem Geschäftsmodell im Zusammenhang stehenden Funktionalität undenkbar. Im Bereich „nur" des Datenschutzes schien dies nicht so wichtig zu sein.

Fall 41: Schweigen ist Gold

Praktischer Fall: Die Müller Bank AG weist auf Kontoauszügen für ihre Kunden, wenn Zahlungen auf deren Konten bei der Müller Bank AG eingehen, die Adresse des Zahlenden aus. Ist diese Vorgehensweise datenschutzrechtlich zulässig?

Dieser Fall geht auf einen Bußgeldbescheid der rumänischen Datenschutzaufsicht vom Juli 2019 zurück. Sie wirft viele Folgefragen in Richtung „wer darf welche Daten einsehen?" auf, und zwar sowohl bei rein unternehmensinterner Betrachtung („*need to know*", dazu schon oben Fälle 3, 6, 21 und 27) als auch bei der Übermittlung bzw. „Zurverfügungstellung" von Daten an Dritte. Wichtig ist dabei, dass nach Art. 4 Nr. 2 DSGVO eine „Verarbeitung" personenbezogener Daten (auch) durch „*die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung*" erfolgt. Und diese Verarbeitungshandlung benötigt – wie jede andere auch – eine Legitimationsgrundlage und muss sich an den grundlegenden Prinzipien des Art. 5 DSGVO messen lassen.

Die rumänische Behörde war der Ansicht, dass die Adresse des Zahlenden, auch wenn dieser der verbuchenden Bank selbst (warum auch immer) legitimerweise vorliegt, von der Bank nicht an ihren Kunden – durch Anzeige in den Umsätzen (Transaktionsdetails) – offengelegt werden darf. Dies verstoße gegen Art. 5 Abs. 1 lit. c) DSGVO, den Grundsatz der Datenminimierung. Die Weitergabe der Adresse des Überweisenden bzw. Einzahlers (also eines dritten Betroffenen) ist für die Zwecke des (Girokonto-) Vertrages zwischen Bank und Kunden nicht erforderlich. Der Kunde benötigt diese Adresse nicht, um nachvollziehen zu können, dass ihm eine Zahlung von diesem Dritten geleistet wurde. Im Fall der rumänischen Datenschutzaufsicht ging es immerhin um 337.024 Betroffene (Dritte) im Zeitraum zwischen dem Inkrafttreten der DSGVO und dem 10. Dezember 2018, als diese Praxis gestoppt wurde.

Ob dies immer und uneingeschränkt gilt – z. B. wenn der Kontoinhaber zwei Zahlungen erwartet von zwei namensgleichen Schuldnern, die er nur anhand der Adresse voneinander unterscheiden könnte –, sei hier dahingestellt. Wichtiger ist, dass bei jeder Zurverfügungstellung von Daten darüber nachgedacht werden muss, warum der Empfänger auf diese Daten einen „datenschutzrechtlich legitimierbaren Anspruch" haben sollte. Nun könnte man natürlich darüber nachdenken, wie es datenschutzrechtlich zu beurteilen wäre, wenn der (Girokonto-) Vertrag zwischen der Bank und dem Kunden die Klausel beinhalten würde, dass zu jeder eingehenden Überweisung dem Kunden die der Bank dazu vorliegenden Daten – also auch die Adresse des Zahlenden – zur Verfügung gestellt werden. Dann wäre die Über-

mittlung nach diesem Vertragsinhalt „erforderlich“. Dies kann ggf. zur „datenschutzrechtlichen Inhaltskontrolle“ des (Girokonto-) Vertrages führen; dieser kann nicht einfach „alles“ datenschutzrechtlich legitimieren (s. oben Fall 30).

Doch der Kreis ist noch weiter zu ziehen: Auch irgendwo „liegengelassene“ Daten werden allen potenziell technisch Zugriffsberechtigten „offengelegt“. Hätte die Bank etwa die Adressen sämtlicher Zahlender intern in Form eines Excel-Exports auf einem Netzlaufwerk abgelegt, auf das sämtliche Bankmitarbeiter Zugriff haben, so hätte eine Offenlegung der Daten – durch „Bereitstellung“ – an sämtliche Bankmitarbeiter und damit auch an Unbefugte (die kein „*need to know*“ haben) stattgefunden. Dies zeigt die „unternehmensinterne“ Dimension bei einer „Weitergabe“ von Informationen.

Plausibler mag im Hinblick auf eine interne Offenlegung der Fall sein, dass im Rahmen einer IT-Migration von Stammdaten der Beschäftigten (von einem System auf ein anderes) sämtliche Stammdaten der Beschäftigten eines Unternehmens in einem generell als „Transferverzeichnis“ genutzten Netzlaufwerk „zwischengeparkt“ werden. Wenn dies erst einige Zeit später auffällt, mag es sein, dass unbefugte Mitarbeiter (d. h. nicht aus der IT-Abteilung, soweit mit dem Migrationsprojekt befasst, und nicht aus der Personalabteilung, soweit mit den Stammdaten befasst) Einsicht in die Datei genommen haben. Dies könnte sogar nicht nachvollziehbar sein, weil Lesezugriffe nicht protokolliert werden (s. zur Frage der Pflicht zur Protokollierung von Lesezugriffen oben Fall 38). In derartigen Fällen, in denen Daten Unbefugten zur Verfügung standen, aber unklar ist, ob die Unbefugten tatsächlich die Daten eingesehen haben, steht ein Datenschutzverstoß – die „Bereitstellung“ ohne Legitimationsgrundlage – fest. Offen aber ist, ob ohne Möglichkeit des Beweises für oder gegen die erfolgte Einsichtnahme – die Beschäftigten, denen der Zugriff möglich gewesen wäre, kann man nicht fragen, da diese die Einsichtnahme wohl nicht zugeben würden – im Rahmen einer Meldepflicht nach Art. 33 DSGVO davon ausgegangen werden darf, „*dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt*“ (s. dazu auch oben Fall 35). Die Beantwortung dieser Frage hängt entscheidend davon ab, ob ein Zugriff stattgefunden hat – dann wären ggf. auch die Betroffenen zu benachrichtigen (Art. 34 DSGVO) – oder nicht – dann bestünde kein Risiko für die Betroffenen. Im Zivilprozess fragt man in diesen Fällen, deren Sachverhalt letztlich nicht zur Überzeugung des Gerichts ermittelt werden kann, wer die Beweislast trägt. Die Formulierung „*es sei denn*“ in Art. 33 DSGVO würde nach diesem (für EU-Verordnungen aber nicht anwendbaren) Maßstab darauf hinweisen, dass im Zweifel – also wenn nicht nachgewiesen werden kann, dass keine Einsichtnahme stattgefunden hat – zu melden ist.

Neben die Frage des Datenschutzverstoßes tritt natürlich die Frage, wann die Betroffenen Schadensersatzansprüche (Art. 82 DSGVO) geltend machen können. Hierfür könnte die Frage, ob Dritte tatsächlich auf die Daten zugegriffen haben, entscheidend sein (s. oben Fall 9).

Schlusswort

Unabhängig davon, was juristische Experten so alles glauben oder noch glauben werden, aus dem Orakel von Delphi – der DSGVO – eindeutig herauslesen zu können: Es macht den Anschein, dass alltägliche Situationen, denen sich mittelständische Unternehmen ausgesetzt sehen, vom „Gesetzgeber" (wer immer das konkret sein mag) im Vorfeld des Gesetzeserlasses nicht besonders durchdacht wurden. Es wäre ein Leichtes gewesen, diese Situationen zu identifizieren und konkret im Text zu regeln, um der Praxis klar und bestimmt aufzuzeigen, was erlaubt und was verboten ist. Schließlich erwartet der Gesetzgeber auch klare Anweisungen der Unternehmen an ihre Mitarbeiter, was sie zu tun und zu lassen haben. Diese Chance wurde vertan und die Interpretationsrisiken auf die Unternehmen abgewälzt. Auch wenn die DSGVO bisweilen sinngemäß darauf hinweist, dass auf die besonderen Bedürfnisse kleinerer und mittlerer Unternehmen Rücksicht zu nehmen ist, weiß niemand, was diese politischen Sätze konkret bedeuten sollen. Es bleibt auch im Dunkeln, was das bayerische Landesamt für Datenschutzaufsicht im Tätigkeitsbericht 2017/2018 im Kontext einer noch nicht abgeschlossenen eigenen Untersuchung meint, wenn ausgeführt wird, dass die Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) bedeute,

„dass die Einhaltung der gesetzlichen Anforderungen der Aufsichtsbehörde bei einer Kontrolle dargestellt werden muss. Während dies bei großen Unternehmen in der Regel nur anhand einer systematischen Ausgestaltung der Geschäftsprozesse erreicht werden kann, skaliert die DSGVO bei kleinen und mittleren Unternehmen recht gut. Die Einhaltung der datenschutzrechtlichen Anforderungen kann deutlich weniger formal erreicht werden".

Eher dürfte auf der Hand liegen, dass die in den obigen Fallkonstellationen aufgeworfenen Fragestellungen mit erheblichen Haftungsrisiken versehen sind – gleich ob bei kleineren und mittleren Unternehmen oder bei Großunternehmen –, denn juristische Probleme haben die Eigenart, in ihrer Komplexität nicht von der Größe von Unternehmen oder von der Höhe eines Geldbetrages abhängig zu sein. Wenn man mit seiner Antwort auf der „falschen Seite" liegt, besteht das Risiko, dass Daten unrechtmäßig verarbeitet oder Pflichthinweise falsch gegeben werden – mit den bekannten Folgen für sämtliche Verantwortlichen, allenfalls noch mit unterschiedlicher „Schwere der Schuld". Mit dem üblichen *„hindsight bias"* – auf gut deutsch: Nachher ist man immer schlauer – wird so mancher, wenn eines Tages ein (höchstes) Gericht so oder so entscheiden wird, sagen, dass man das immer schon hätte wissen müssen, denn die Gerichtsentscheidung sei doch klar absehbar gewesen. Man muss sich dann mit dem Gedanken aus der Compliance-Haftung behelfen, dass bei unklarer Rechtslage nach Abwägung von jeglichem Für und Wider das Unternehmen berechtigt ist, die für das

Unternehmen günstigere Lösung zu wählen. Ob das auch im europarechtlichen Kontext der DSGVO gilt, bleibt abzuwarten. Zwar sagen die Juristen unter Hinweis auf die zum Teil sehr unbestimmten Regelungen, dass es „in der ersten Zeit der Anwendbarkeit der DSGVO Einzelfälle geben kann, in denen auch unter Berücksichtigung der strengen Rechtsprechung des EuGH und des Europäischen Gerichtshofs für Menschenrechte eine Sanktionierung mangels Vorhersehbarkeit ausgeschlossen ist“ (Bergt, DuD 2017, 555, 560). Das verschiebt das Problem jedoch nur von der „Unbestimmtheit“ der DSGVO selbst auf die „Unvorhersehbarkeit“, wie die (vielen) Würfel fallen, welche die DSGVO unbestimmt in die Luft geworfen hat und welche noch einige Jahre fliegen werden. Und was heißt „in der ersten Zeit der Anwendbarkeit“? Rechtssicherheit können die derzeit „guidance“ um „guidance“ produzierenden Aufsichtsbehörden ebenso wenig schaffen wie die Finanzverwaltung im Bereich des Steuerrechts. Es ist – wie immer – Zufall, welche konkreten Rechtsfragen am Ende tatsächlich mit enormem Geldeinsatz bis zum EuGH „durchgepeitscht“ werden, um sich im Nachgang zur Gesetzgebung und zu den Interpretationsversuchen der Exekutive punktuelle Rechtssicherheit einzukaufen. Selbst in altehrwürdigen Rechtsmaterien wie dem Handelsgesetzbuch sind so manche große Rechtsfragen bis heute nicht höchstrichterlich entschieden worden, weil „die Wirtschaft“ zu häufig davon abgesehen hat, zur Lösung eines Konflikts, den der Gesetzgeber in mittlerweile weit über 100 Jahren nicht lösen wollte, noch gutes Geld dem schlechten hinterherzuwerfen.

Wenn der Gesetzgeber die Sorgfalt, die er von den Gesetzesanwendern erwartet, selbst hätte walten lassen, sähe die Sache deutlich anders aus. Von daher erscheint es unangemessen, die Schuld – wie oft versucht wurde – auf die Berater abzuschieben, die nur die Überbringer der schlechten Nachricht sind. Die Einführung einer Haftung wegen „mangelhafter Gesetzestexte“ wird der Gesetzgeber wohl zu verhindern wissen. Schließlich sind Rechtsanwender – in diesem Fall die Unternehmen – und Gerichte leidensfähig und als solche keine Wähler.

Anhang

In diesem White Paper wurde die Unbestimmtheit vieler Passagen und Begriffe der DGSVO kritisiert. Besonders gefährlich für den Rechtsanwender ist dabei, dass die Nichteinhaltung dieser unbestimmten Vorgaben mit drastischen Sanktionen verknüpft werden. Wenn man sich zum Vergleich Gesetzestexte vorstellt wie „Wer sich ungut verhält, wird geköpft" oder sogar „Wer sich nicht gottgefällig verhält, wird geköpft", erzeugt dies ein Gefühl des Unbehagens – ein Rückfall in „düstere" Zeiten ist zu befürchten. Vor diesem Hintergrund lohnt es sich durchaus, auf Basis des nachfolgenden Exkurses – als Polemik und Denkanstoß verfasst – über die Hintergründe und Auswirkungen gesetzlicher Unbestimmtheiten sowie über die Einordnung der DSGVO in das Rechtssystem insgesamt nachzudenken. Denn je besser ein Gesetz „gemacht" ist – was immer das heißt –, desto besser kann es angenommen (verinnerlicht) und befolgt werden. Dahinter steht nichts weniger als die Frage, was das „Primat des Rechts" als Wesenskern eines (gewaltengeteilten) „Rechtsstaats" im Kontext einer modernen, hyperkomplexen Welt eigentlich bedeutet. Das Nachdenken lohnt sich – sapere aude!

Wer „macht" eigentlich Recht?

Für den Rechtsanwender, der nicht selbst Lobbyarbeit in Berlin oder Brüssel betrieben oder an Expertenanhörungen oder Ausschusssitzungen teilgenommen hat, fallen Gesetze praktisch vom Himmel bzw. stehen auf einmal in einem Gesetzblatt. Dann beginnt der Wesenskern der Arbeit eines Juristen: die Auslegung des Gesetzestextes. Für den juristischen Laien mutet das wie eine Geheimwissenschaft an, denn allzu oft zaubern Juristen als Auslegungsergebnis das sprichwörtliche Kaninchen aus dem Zylinder. Das ist bei der Auslegung bzw. den Auslegungsergebnissen kirchlicher Texte und deren gleichnishaften und „zeitlosen" Handlungsanweisungen nicht anders. Dass die Juristen die „Kaninchenhaftigkeit" ihrer Ergebnisse selbst nicht immer bemerken, liegt daran, dass nun einmal jeder in seiner eigenen Welt („Sinnblase") lebt und der „Blick über den Tellerrand" von dort aus oft nicht nur ungewohnt, sondern mit erheblichem weiteren Aufwand verbunden ist. Das beginnt schon bei dem juristischen Sprichwort „Das Gesetz ist klüger als der Gesetzgeber", landläufig auch „Das Ei ist klüger als die Henne". Dieser für den Laien gewöhnungsbedürftige Gedanke geht ursprünglich auf den Philosophen Immanuel Kant zurück, der 1787 schrieb, es sei nicht ungewöhnlich, einen Verfasser „sogar besser zu verstehen, als er sich selbst verstand, indem er seinen Begriff nicht genugsam bestimmte und dadurch bisweilen seiner eigenen Absicht entgegen redete oder auch dachte". Nach der überaus klugen Vorschrift des § 133 BGB ist denn auch bei der Auslegung von Erklärungen „der wirkliche Wille zu erforschen und nicht

an dem buchstäblichen Sinne des Ausdrucks zu haften“. Und bereits Cicero zitierte einen schon damals lange bestehenden Satz, dass durch böswillige und spitzfindige Interpretation, die sich nur an den Buchstaben des Rechts, nicht aber an Sinn und Intention orientiert, aus „Recht“ ein „Unrecht“ werden kann. Das klingt zusammengenommen so, als gebe es einen „wirklichen“ Willen (Absicht) des Gesetzgebers, der unter „nicht genugsam bestimmten Begriffen“ verschüttet wurde und nun von einer Heerschar von „geheimbündlerischen Juristeninterpreten“ mit Hammer und Meißel freigelegt werden muss. Für den Laien dürfte das eine seltsame Vorstellung sein: Kann man nicht gleich den Sinn und die Intention unmissverständlich in Buchstaben niederlegen?

Hinzu kommt die „Zwitterstellung“ der Erwägungsgründe von EU-Verordnungen und EU-Richtlinien sowie der Gesetzesbegründungen nationaler Gesetze. Sie sind selbst kein Gesetzestext, dürfen nach Ansicht des EuGH auch nicht dazu führen, dass das Gesetz entgegen seinem Wortlaut interpretiert wird, stellen aber trotzdem ständig bemühte „gesetzgeberische Auslegungshilfen“ dar. Man stelle sich vor, das Gesetz „Wer sich ungut verhält, wird geköpft“ würde durch 200 Erwägungsgründe eingeleitet, in denen punktuell darauf hingewiesen wird, was der Gesetzgeber „beispielsweise“ oder „im Grundsatz“ als ungut ansieht. Gerichte würden dann das Gesetz (natürlich) entsprechend der Erwägungsgründe auslegen – sie sind um jede Auslegungshilfe dankbar –, gleichzeitig aber immer darauf hinweisen, dass das natürlich kein Gesetzestext und daher mit Vorsicht zu genießen ist. Der Laie wird das zumindest eigentümlich finden. Warum teilt der Gesetzgeber den Text, den er als Gesetz verabschiedet, in „eigentlichen“ und „uneigentlichen“ Text ein, von dem der eine gilt und der andere „irgendwie so halb“?

Gutes Recht zu schaffen fordert einem Gesetzgeber enorme Anstrengungen ab, um Absichten klar zu definieren und möglichst für die Adressaten verständliche, unmissverständliche Begriffe auf dieser Basis zu formulieren. Das BGB beispielsweise beruht auf dem im 19. Jahrhundert in jahrzehntelanger Vorarbeit entwickelten Anspruch, eine fein ausziselierte Rechtsordnung mit großer innerer Folgerichtigkeit zu entwickeln. Die Grundgedanken dazu stammen aus dem römischen Recht, dem ein hoher Grad an Abstraktion und Systematik zugrunde lag. Man nennt das heute eher abfällig „Begriffsjurisprudenz“, obwohl doch auch attestiert wird, dass diese Vorgehensweise „sorgfältige Kleinarbeit“ geleistet und dabei die bisweilen kompliziertesten und am schwierigsten zugänglichen, gleichwohl aber gründlich durchdachten Rechtsfiguren des bürgerlichen Rechts geschaffen hat. Vorherige („altdeutsche“) Gesetzbücher waren demgegenüber eher eine Aneinanderreihung von sehr konkreten einzelnen Wenn-Dann-Vorgaben.

Die damals „neue“ Vorgehensweise des BGB bedeutete einerseits, dass der Umgang mit dem Gesetz vor allem den besonders geschulten Juristen überlassen wurde. Andererseits sollte so die Willkür des Richters gegenüber den streitenden Parteien möglichst eng begrenzt werden. Daraus entwickelte sich das ewig expandierende Universum juristischer Sekundärliteratur, gestützt auf die juristische Methodenlehre der Auslegung nach historischen, systematischen, zweckorientierten und wortlautgetreuen Gesichtspunkten. So wichtig in der kontinentaleuropäischen Rechtskultur Gerichtsentscheidungen sind, so wichtig sind auch juristische Kommentierungen. Denn Gerichtsentscheidungen haben „nur“ den Anspruch, einen konkreten Fall anhand des einschlägigen Gesetzestextes und ggf. der vom Richter „erkannten“ (Begriffs-) Systematik dahinter zu lösen. Die Systematik muss also vom Richter nur insoweit „erforscht“ werden, als dies für die Lösung des konkreten Sachverhalts notwendig ist und der Gesetzestext nicht einfach subsumierbar ist (wobei in diesem Fall wohl nur Querulanten einen Richter bemühen würden). Wie oft schon hat man sich als Rechtsanwender beim Lesen einer Gerichtsentscheidung aber gefragt, wie denn nun ein leicht abgewandelter Fall zu lösen wäre – aber dazu musste sich das Gericht ja nicht äußern. Diese Aufgabe, die Systematik „hinter“ und „zwischen“ dem Gesetzestext umfassend und möglichst widerspruchsfrei zu ergründen – oder erst zu definieren –, ist Aufgabe juristischer Kommentarliteratur, von Doktorarbeiten, Zeitschriftenartikeln, Blogs und sonstigen Sekundärquellen. Jedes neue Gesetz verursacht einen regelrechten „Run“ auf die Unschärfen und Auslegungsprobleme, die Druckpressen rattern und das Internet brummt, und irgendwann heißt es mit Karl Valentin: „Es ist schon alles gesagt worden, nur noch nicht von jedem“. Anerkennung und Aufmerksamkeit sind die wesentlichen Triebfedern menschlichen Handelns – das gilt auch für Juristen. Durch diesen immer größer gewordenen „Gesetzesverdauungsapparat“ konnte die historische Absicht des Gesetzgebers, ein möglichst konsistentes und „weises“ Rechtssystem bereitzustellen, nahezu unbemerkt aufgegeben werden. Neuere Gesetze – auch und vor allem auf EU-Ebene – sind nicht das Produkt einer ausgiebigen Begriffsforschung, sondern, wie es der Philosoph Peter Sloterdijk einmal sinngemäß formulierte, das Ergebnis des Handelns von „parlamentarischen Erpressergruppen“, die Themen bzw. Textvorschläge der Ministerialbürokratie ohne inhaltlichen Zusammenhang zu (mitunter faulen) Kompromissen miteinander verknüpfen und dabei Textänderungen ohne ausreichenden Sachverstand bzw. Konsistenzkontrolle vornehmen. Was für ein Glück, dass in Parlamenten – im Gegensatz zur DSGVO – kein Koppelungsverbot gilt.

Recht wird also von einem Gesetzgeber und von Interpretationsjuristen (einschließlich Richtern) geschaffen. Auslegung ist Rechtsschöpfung, nicht nur Rechtsanwendung; wäre sie nur Rechtsanwendung, könnte man sie längst den Computern überlassen, die das Recht viel schneller „durchrechnen“ könnten. Viele Juristen sagen auch heute noch „Diese Norm muss

so ausgelegt werden, weil sich das aus dem Gesetz so ergibt“, obwohl sie meinen: „Ich würde die Lücken in dieser Norm so auffüllen, wenn ich der Gesetzgeber wäre“. Und wenn die Lücken (inklusive begrifflicher Unschärfen) dann tatsächlich von einem Gericht so aufgefüllt werden, wurde neues Recht geschöpft, nicht nur bestehendes Recht interpretiert. Der große Jurist Gustav Radbruch formulierte dies 1906 mit unnachahmlicher Präzision so: „Rechtsprechung und Rechtswissenschaft sind trotz der Gewaltenteilungslehre immer rechtsschöpferisch geblieben und werden es immer bleiben und nur darin unterscheidet sich der heutige vom ehemaligen und hoffentlich auch vom künftigen Juristen, dass er verbirgt, was jene offen zugestehen“.

Die Illusion des „mathematischen Rechts“ – Begriffsgummi statt Präzisionsformeln

Jede Rechtsschöpfung arbeitet mit abstrakten Begriffen und stößt dabei an begriffliche Grenzen. Die juristische Subsumtion als Test, ob ein bestimmtes „Sein“ (Sachverhalt) einem bestimmten „Sollen“ (Rechtsnorm) entspricht oder nicht, ist immer eine Frage der (subjektiven) Überzeugung, ob sich die beiden Ebenen decken oder nicht. Das eine kann sich nicht aus dem anderen „mathematisch“ ergeben, weil Realität (Sein) und Normen (Sollen) aus zwei unterschiedlichen Welten stammen – Normen sind begriffliche Inhalte in einer ganz speziellen virtuellen Laufzeitumgebung, nämlich dem „Rechtssystem“, Realität hingegen sind alle anderen (physikalischen oder virtuellen) Laufzeitumgebungen. Man könnte dies umgangssprachlich auch so fassen, dass die Juristen darin Meister sind, abstrakte Begriffe durch andere abstrakte Begriffe zu ersetzen, um irgendwann durch genügend „vordergründige Schein-Präzisierung“ (Rhetorik) die Illusion einer perfekten Deckungsgleichheit zwischen Realität und Norm zu schaffen.

Auf den überaus klugen Aristoteles geht etwa die logische Schlussfolgerung zurück „Wenn alle Menschen sterblich sind und alle Griechen Menschen sind, dann sind alle Griechen sterblich“. Wenn das mal so einfach wäre. Die Begriffe „Mensch“, „sterblich“ und „Griechen“ sind 2300 Jahre danach nicht mehr so eindeutig, wie sie es einmal waren. Sind Cyborgs Menschen? Heißt sterblich auch einfrier- und wieder auftaubar? Sind aus Griechenland ausgewanderte Griechen immer noch Griechen? Man könnte also umformulieren: „Wenn alle Lebewesen, die überwiegend aus menschlichen Zellen bestehen, bei irreversiblen Hirnschäden nicht mehr bewusstseinsaktiviert werden können, und alle Personen, die griechischer Abstammung sind, Lebewesen sind, die überwiegend aus menschlichen Zellen bestehen, dann können alle Personen, die griechischer Abstammung sind, bei irreversiblen Hirnschäden nicht mehr bewusstseinsaktiviert werden“. Man muss sich nicht vertieft mit analyti-

scher Sprachphilosophie oder juristischer Hermeneutik beschäftigt haben, um hier das Problem zu benennen: Durch die Umformulierung wird der Satz alles andere als – wie ursprünglich beabsichtigt – „mathematisch präzise". Der Grund dafür ist einfach: Begriffe sind letztlich soziale Übereinkünfte und diese sind nicht präzise (bzw. wahr oder falsch), sondern bilden einen Graukeil dessen, auf das man sich mehr (sog. „Begriffskern") oder weniger (sog. „Begriffshof") einigen kann. Dies gilt schon für Begriffe, die einfache Dinge benennen – man muss also nicht gleich solche „Monsterbegriffe" wie „Angemessenheit" oder „Stand der Technik" bemühen: Wenn das Kind mit einem Finger auf ein „Ding" zeigt und die Mutter „Auto" sagt, dann ist das für das Kind ein Auto, selbst wenn es sich für viele andere um einen Lastwagen handelt – im Gegensatz zu einem anderen Kind, dem vielleicht ein Motorrad mit Beiwagen als Auto benannt wurde. Und mit je mehr Begriffen man hantiert – und je abstrakter diese sind –, desto mehr Graukeile werden bis zur Unkenntlichkeit aufeinandergetürmt. Würde also der überaus kluge Aristoteles nun Art. 26 Abs. 1 S. 1 DSGVO subsumieren, so würde er sagen: „Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. A ist ein Unternehmen und beauftragt den Wirtschaftsprüfer B mit der Prüfung des Jahresabschlusses in seinem Hause. A und B sind also ..." – Tja, so einfach ist es dann doch nicht.

Ob eine Karosserie auf drei Rädern „schon" unter den Begriff des Autos oder „noch" unter den Begriff des Motorrads zu subsumieren ist, ist schlicht Definitionssache – das kann man, wie Juristen so schön sagen, so oder so sehen. Wenn nun der Gesetzgeber ein Gesetz ersinnt und es „da draußen" vor dreirädrigen Karosserien nur so wimmelt, dann hat er vordergründig zwei Möglichkeiten. Entweder er definiert „Auto" mit vier Rädern und „Motorrad" mit zwei Rädern und überlässt es „der Praxis" – also den geheimbündlerischen Juristen –, dieses Orakel für die Dreirädrigkeit zu lösen. Man könnte das fast als böswillig bezeichnen, aber mutmaßlich handelt es sich nur um einen „politischen Kompromiss", weil sich die Fraktionen über die Einordnung nicht einig wurden, oder Parlamentarier fahren nur in vierrädrigen Dienstlimousinen und schauen währenddessen auf ihre Akten. Oder der Gesetzgeber schreibt ins Gesetz, wie eine Karosserie mit drei Rädern konkret einzuordnen ist. Dann hat er zwar mindestens einen Doktoranden um dessen Doktorarbeit gebracht, ansonsten aber Rechtssicherheit für die dreirädrigen Gefährte „da draußen" geschaffen. Dies ins Gesetz zu schreiben bedeutet aber, dass man alle relevanten Dinge „da draußen" aufmerksam beobachtet hat und sich dann darüber klar werden muss, dass und wie man es nun regeln will und welche Konsequenzen es hätte, wenn dann bei einer Einordnung als „Auto" – gemäß den dort geltenden Regeln – alle dreirädrigen Karosserien über zwei Front- und zwei Schlusslichter verfügen müssten.

Der DSGVO-Gesetzgeber hätte in diesem Bild noch einen dritten Weg beschritten; er hätte geschrieben: „Hat ein Objekt einen auf Fortbewegung gerichteten Zweck, so müssen die Mittel der Beleuchtung angemessen sein." Das klingt ungefähr genauso gut wie „Wer sich ungut verhält, wird bestraft" (wer würde das nicht wollen?), sagt aber weniger aus als z. B. dass konkret für jedes Rad an einer Karosserie ein Front- oder Schlusslicht angebracht werden muss. Diese ergänzende Rechtsschöpfung bleibt hier der „Praxis" vorbehalten, die sich dann darauf beruft, das Recht „nur ausgelegt" zu haben. Zusätzlich wird es dann auch lange juristische Artikel über das Wort „Zweck" und das Wort „Mittel" im genannten Satz geben. Und der Gesetzgeber würde sich rühmen, das Problem allgemein gelöst zu haben: Er war so „klug", sogar fünf- und sechsrädrige Gefährte ohne Karosserie sowie Flugtaxis vorhergesehen und geregelt zu haben! Das zeigt anschaulich das Dilemma: Der Gesetzgeber ist nicht so „klug", alle Fallgestaltungen vorherzusehen, die die unvorhersehbare Realität ersinnt, möchte sie aber eigentlich alle regeln, selbst wenn er nicht wissen kann, ob die Regelung für alle möglichen zukünftigen Fallgestaltungen „fair" ausfällt. Die Bestimmtheit muss dabei auf der Strecke bleiben.

Was haben Sie für Interessen und Werte?

Da das BGB als Paradebeispiel der Begriffsjurisprudenz sehr sperrig ausgefallen ist – es hat zwar weit über 100 Jahre ganz gut funktioniert, aber dennoch häufig Rechtsfortbildung erfordert –, wurde die Interessenjurisprudenz entwickelt. Letztlich dient Recht ja der Ermöglichung eines gedeihlichen Zusammenlebens von Menschen, muss also Interessenkonflikte friedlich schlichten. Jeder Mensch – oder besser: jeder am Rechtsverkehr Teilnehmende – darf sein Interesse in die Waagschale werfen, dann wird abgewogen, und dann „gewinnt" eine Seite, die „im Recht" ist. Üblicherweise würde man davon ausgehen, dass der Gesetzgeber selbst diese Interessen abstrakt bewertet und so den Ausgang der Interessenabwägung „normiert". Zumindest möchte man dem Gesetzestext Hinweise darauf entnehmen können, wie der Gesetzgeber Interessen gegeneinander abwägt, um dann für ähnliche Fallgestaltungen, die nicht direkt von einer Gesetzesnorm erfasst werden, einen Hinweis auf das „richtige" Abwägungsergebnis extrapolieren zu können. Noch abstrakter als Interessen sind „Werte", an denen sich die Gesetzesauslegung orientieren kann. Die Interessenjurisprudenz wurde so später zur Wertungsjurisprudenz ausgebaut, die neben den Ergebnissen gesetzgeberischer Interessenabwägungen auch Raum für selbst dem Gesetz(geber) übergeordnete „Gerechtigkeitselemente" wie universelle Menschenrechte, Grundrechte etc. lässt.

Der Gesetzgeber schreibt aber in Art. 6 Abs. 1 S. 1 lit. f) DSGVO, dass personenbezogene Daten verarbeitet werden dürfen, soweit „die Verarbeitung zur Wahrung der berechtigten

Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen". Er überlässt also die Frage, welche Interessen überhaupt legitimerweise bestehen können und wie diese dann untereinander abzuwägen sind, dem Gesetzesanwender, d. h. letztlich den Gerichten. Selbst ein Wertungsmaßstab für die Interessenabwägung lässt sich dieser Norm kaum entnehmen. Der Bundesgerichtshof hat dies in einer Entscheidung vom Juli 2018 freundlich so umschrieben, dass die in der DSGVO genannten, sehr punktuellen Beispiele für berechtigte Interessen „zeigen, dass vielfältige und unterschiedlich bedeutsame Interessen berücksichtigungsfähig sind", und dass nicht nur „zwingende rechtliche Interessen", sondern auch ein „ideelles Interesse im Rahmen der Abwägung berücksichtigungsfähig" ist. Gerade im Datenschutzrecht wird das, was eigentlich der Gesetzgeber und die öffentliche Verwaltung machen sollten – Grundrechte bzw. Grundrechtseingriffe gegeneinander abwägen –, zunehmend auf sämtliche Adressaten (nun also die DSGVO) abgewälzt. Diese Adressaten würden lieber klare Verhaltensregeln („dos and don'ts") vor sich haben als sich nun mit diffizilen Grundrechts- und Interessen-Abwägungsfragen herumplagen zu müssen, die an sich „Spielwiese" der Verwaltungs- und Verfassungsjuristen sind und die man „so oder so" sehen kann. Mit „Drittwirkung der Grundrechte" bezeichnet man kurz gesagt das „Hineinquellen" von Grundrechtsfragen durch unbestimmte Rechtsbegriffe wie „Treu und Glauben" in die privatrechtlichen Beziehungen zwischen Privatrechtssubjekten (Bürgern bzw. Unternehmen) untereinander. Was in der Vergangenheit die Ausnahme war, wird nun zur Regel: Das „verantwortliche" Unternehmen wird im Datenschutzrecht zur Behörde umfunktioniert, die gegenüber dem „Bürger-Betroffenen" Grundrechte abwägen und Grundsätze des Verwaltungsverfahrens einhalten muss.

Eigentlich könnte man diese Gedanken auch konsequent fortführen und das bisherige Recht durch ein „Master-Gesetz" ersetzen, das nur aus einer Regelung besteht: „Das Gericht soll die verschiedenen Interessen der Beteiligten ermitteln und abwägen und dann bestimmen, wer was darf. Sollte das Gericht dabei zur Gewichtung der Einzelinteressen auf Wertungsmaßstäbe zurückgreifen müssen, dann möge es die nehmen, die es nach dem übereinstimmenden Verständnis aller billig und gerecht Denkenden schon immer gab, oder wie sie sich im Laufe der Zeit eben gewandelt haben, wie etwa auch Grund- und Menschenrechte, kurzum: Das Gericht möge sich allen Beteiligten gegenüber fair verhalten." Ein bisschen so funktionierte ja schon früher das „common law" der angloamerikanischen Rechtssphäre und viele Richter werden in den USA nach wie vor vom Volk gewählt. Aber es klingt nicht gerade nach einer Vorhersagbarkeit der Entscheidungen – als (wichtige) Facette des Begriffes „Rechtsstaat" –, sondern in heutigen Zeiten eher nach einer Kapitulation des Gesetzgebers vor der in Geschwindigkeit und Ausmaß exponentiell wachsenden Komplexität unserer

Welt. Man könnte es für den Gesetzgeber auch so formulieren: Je mehr ein Richter täglich vor Ort entscheiden kann, desto weniger müssen wir in unserem Parlament alle paar Jahre entscheiden, wenn das Gesetz mal wieder turnusmäßig oder anlassbezogen auf den Revisionsprüfstand muss. Na denn: Hoffentlich entscheidet der Richter auch wirklich autonom und schreibt nicht nur in aller Eile das ab, was Kommentatoren zuvor voneinander abgeschrieben haben oder was Aufsichtsbehörden zum Gesetzestext „hinzuinterpretiert" haben.

Apropos Parlament: Die aufgrund der DSGVO notwendige Revision des Rechts des Sozialdatenschutzes im Sozialgesetzbuch – das Sozialgeheimnis geht immerhin auf die Reichsversicherungs-Verordnung aus dem Jahr 1911 zurück – wurde in einem „Omnibusgesetz" („Alle einsteigen!") gleichsam „versteckt". An ein Gesetz zur Änderung des Bundesversorgungsgesetzes wurden u. a. die entsprechenden Änderungen der datenschutzrechtlichen Regelungen des Sozialgesetzbuches (SGB) angehängt und so nahmen weder die breite Öffentlichkeit noch die Fachöffentlichkeit Notiz. Am Ende einer ganztägigen Plenarsitzung stimmte der Bundestag nach Mitternacht noch schnell ohne Debatte diesem Gesetzespaket „im Hinausgehen" zu. Der Bundesrat kritisierte diese Vorgehensweise, ließ das Gesetz aber ebenfalls in seiner letzten Sitzung vor der Sommerpause 2017 passieren. Das Resultat ist traurig: Eine oberflächliche, kaum erhellende Gesetzesbegründung, eine unverständliche Regelung zum Verhältnis des Sozialdatenschutzes zur DSGVO und viele weitere ungelöste Probleme. Immerhin muss angefügt werden, dass der nächste gesetzgeberische Flicken auf diesem Teil des Datenschutzteppichs schon auf dem Weg ist. Eine mit der Komplexität der Materie ringende Ministerialbürokratie bahnt sich ihren Weg durch das große Maisfeldlabyrinth des Datenschutzes.

So erhellend das alles sein mag, um das Problem zu verstehen, so wenig vermag es zur Lösung selbst beizutragen. Der Gesetzgeber wird in Zukunft – d. h. im nie versiegenden Strom der Gesetze, Richtlinien und Verordnungen – nicht mehr besser werden, denn die programmatische Unbestimmtheit hat sich als überaus praktisch erwiesen. An „Wertungsmaßstab" kann man aus der DSGVO wenig mehr herauslesen als dass der Betroffene die „heilige Kuh" des Datenschutzrechts ist. Das führt häufig dazu, dass der Gesetzesadressat – etwa ein mittelständisches Unternehmen – den Kopf in den Sand steckt: Teilweise kennt er die Gesetze nicht, die da so wasserfallartig einprasseln und ihm allerlei präventive Handlungspflichten auferlegen, teilweise will er die Gesetze gar nicht genauer kennen („was ich nicht weiß, macht mich nicht heiß"), weil das alles Althergebrachte in der heilen Welt des Gesetzesadressaten durcheinanderwerfen würde, und vor allem kostet Compliance Geld, mit dem (gefühlt) einzigen Zweck, in der Öffentlichkeit und bei Kunden, Lieferanten und Arbeitnehmern „gut dazustehen". Umsatz oder gar Gewinn bringt Compliance nicht, und

der Gedanke der Reduzierung von Haftungsrisiken setzt ja überhaupt erst einmal voraus, dass es überhaupt ein veritables Entdeckungsrisiko gibt, oder? Also: Je unverständlicher, besser gesagt unbestimmter, ein Gesetz ist, desto wahrscheinlicher, dass es nicht oder feigenblattartig umgesetzt wird. Das beste Feigenblatt ist – plakativ formuliert – der automatische Datenschutzerklärungsgenerator, ein einfaches Muster eines Verarbeitungsverzeichnisses zum Ausfüllen und die Ernennung des Hausmeisters zum Datenschutzbeauftragten. Dann kann man alles andere erst mal so lassen. Hauptsache, das Unternehmen wird nicht irgendwann mit der unternehmensbezogenen Garantie „Das Unternehmen wurde stets im Einklang mit geltenden Rechtsvorschriften geführt" veräußert. Das kann dann teuer werden – Compliance-Einführungskosten als ersatzfähiger Schaden und Vehikel zur nachträglichen Kaufpreisreduzierung.

Was regelt ihr da eigentlich? – Das Datenschutzrecht als universelles Informationsrecht

Nun wäre das alles nicht so schlimm, wenn das Datenschutzrecht wie bisher auch eine „Nischenveranstaltung" im Hinblick auf seine praktische Relevanz geblieben wäre. Das Datenschutzrecht litt schon immer an einer begrifflichen Konturenlosigkeit, an einem eklatanten Vollzugsdefizit und deshalb mangels Überzeugungskraft und Vollzugsdruck („Kontrolldichte") an einer schon immer bestehenden weitgehenden Ignoranz durch die „gemeinen" Rechtsanwender. Wäre es in den vergangenen 30 Jahren vollständig vollzogen worden – so, wie wenn auf jeder Straße alle 50 Zentimeter ein Blitzer installiert würde –, hätte das entweder zu einer Revolution (oder sagen wir zu einem Bauernaufstand) geführt oder aber man hätte die DSGVO als „inkrementelle Weiterentwicklung" klaglos und schulterzuckend in die seit 30 Jahren wie selbstverständlich (weiter-) entwickelten Datenschutz-Compliance-Systeme sämtlicher Vereine, Metzger, Friseure, Ärzte und mittelständischen Unternehmen integriert. Man sollte daher nicht behaupten, die – in ihre Grundfesten relativ unveränderte – Existenz des Datenschutzrechts seit den 1970er-Jahren sei der Beweis dafür, dass das Datenschutzrecht „flächendeckend funktioniert" hat. Allein anhand des rasanten Anstiegs der Sekundärliteratur zur DSGVO – und das ist erst der Anfang der Auslegungsbemühungen – kann geschlossen werden, dass das Datenschutzrecht davor flächendeckend keine besondere Rolle gespielt hat.

Dahinter steckt ein generelles Problem der „inneren Überzeugungskraft" von Recht. Je weiter sich der Gesetzgeber von dem entfernt, was die Gesetzesadressaten – und das kann ein ganzes mittelständisches Unternehmen sein – subjektiv als „vertretbar" empfinden, desto geringer die Motivation, dieses Recht zu befolgen. Dieses Dilemma baut auf zwei Aspekten

auf, dem Aspekt des widersprechenden Rechtsgefühls und dem Aspekt der Unverständlichkeit. Ein „60 km/h"-Schild auf einer geraden, leeren Landstraße bei schönstem Sonnenschein wird jeder Autofahrer als Bevormundung und Gängelung ansehen und in ein Schild uminterpretieren, das wegen der autofreundlichen Umgebung auch bei 100 km/h noch ein Auge zudrückt. Wird der Autofahrer dann bei 90 km/h geblitzt, wird er zwar den formalen Normverstoß nachvollziehen können, den Führerscheinentzug aber als „unfair" bzw. „ungerecht" empfinden. Wird er bei 150 km/h geblitzt, wird er eher einsehen, dass das „eigentlich schon zu schnell" war. Der Fahrer hat also ein eigenes Rechtsgefühl, das er als Maßstab „neben" das Verkehrsschild legt, und wenn die Ergebnisse zu sehr voneinander abweichen, tendiert er dazu, den Normbefehl des Verkehrsschildes für sich zu „verbiegen", ja im schlimmsten Fall als vollständig unverbindlich zu ignorieren. So ist es übrigens auch beim Compliance-Verstoß: Bei vorsätzlichen Regelverstößen spricht das „fraud triangle" neben dem Motiv des Täters und der Gelegenheit für diesen von der persönlichen Rechtfertigung im Sinne von „Das Geld steht mir ohnehin zu" oder „Damit schaffe ich Gerechtigkeit". Auch hier setzt sich der Täter über den Normbefehl hinweg, weil er es „besser weiß". Ähnliches gilt bisweilen auch für die Einführung von (Datenschutz-)Compliance-Management-Systemen insgesamt: Der Aufwand der Einführung (Risikoanalyse, Prozessvorgaben, Kontrolldokumentation etc.) und die absehbaren tiefgreifenden Eingriffe in die gewachsenen oder „liebgewordenen" Unternehmensprozesse führen dazu, dass ein Management die entsprechenden Vorgaben als „weltfremd", sprich: mit dem eigenen Rechtsgefühl nicht vereinbar, ansieht. Dann wird entweder „etwas für die Schublade" produziert, um rein formal das Recht – auch unter Berücksichtigung des als niedrig empfundenen Entdeckungsrisikos – „irgendwie" befolgt zu haben („den Rest sehen wir dann vor Gericht, aber dazu wird es sowieso nicht kommen"). Oder man macht gar nichts – weil man im Laufe der Unternehmensgeschichte schon viele Vorgaben ignoriert hat und damit auch nicht auf die Nase gefallen ist („Der Erfolg gibt unserer Ignoranz Recht").

Das zweite Argument ist die Folge der Überkomplexität der Rechtsordnung selbst: Die Normbefehle haben eine Vernetztheit und Abstraktionshöhe entwickelt, die dem Laien unverständlich ist. Das moderne Recht ist in großen Teilen nicht in der Lage, seine Überzeugungskraft gegenüber den Adressaten aus sich selbst heraus zu schöpen, sondern erst aus den – bei anwaltlicher Beratung für Geldschneiderei gehaltenen – Erklärungen eines Mitglieds einer „Geheimwissenschaft" (d. h. eines Juristen). Jedes normale Kind lernt intuitiv, dass Mord, Vergewaltigung und Betrug etwas ist, „das man nicht macht". Wer sich später weiter im Rechtsverkehr tummelt, wird es irgendwann auch als selbstverständlich empfinden, dass man sich zum Abschluss eines Grundstückskaufvertrags oder für eine GmbH-Grün-

dung zum Notar begeben muss. Aber die vielen unverständlichen Regelungen des Steuerrechts? Des Kartellrechts? Des Datenschutzrechts? Diese Rechtsgebiete kennt man eher als Begriffe aus Film, Funk und Fernsehen und meistens im Zusammenhang mit spektakulären Einzelfällen. Das ist ein Fall für die Rechtsabteilung, wenn es sie gibt, und auch das setzt voraus, dass man die Rechtsabteilung überhaupt einschaltet. Ebenso ist es bei „verrückten" Querbezügen, wenn auf einmal das Datenschutzrecht dazu führt, dass die Haftungsbeschränkungsklausel in den Liefer-AGB unwirksam sein soll. Es gibt dann zu viele Vorgaben, die man nirgends „so" nachlesen kann. Selbst wenn man als Manager die DSGVO am Stück liest, ist es keine Schande, wenn man nach der Lektüre keine Ahnung hat, was das nun bedeuten soll. Wie soll das dann erst der Metzger oder Friseur, der Fußballverein oder der katholische Radiosender verstehen?

Bedauerlicherweise hat das Datenschutzrecht fundamentale Bedeutung in unserer „Informationsgesellschaft". Man sollte sich diese fundamentale Bedeutung, die hier nur kurz umrissen werden kann, immer wieder vor Augen führen. Das Schlagwort „Digitalisierung" beschreibt zunächst einmal nur den Austausch analoger Hardware durch digitale Hardware. Aus einem analogen Telefon, das Sprache mit einem Mikrofon in Spannungsschwankungen umsetzt, überträgt und diese mit einem Lautsprecher wieder in Sprache umwandelt, wird ein digitales Telefon, welches die Spannungsschwankungen eines Mikrofons mittels eines Analog-Digital-Konverters digitalisiert und die digital übertragenen Signale am anderen Ende mittels eines Digital-Analog-Konverters in Spannungsschwankungen für den Lautsprecher umwandelt. Die Digitalisierung führt also zu Informationen, die in digitaler Form vorliegen. Das eigentliche Zauberwort heißt aber „Virtualisierung" und betrifft das, was man mit den digitalen Daten simulieren kann: Aus realem Geld wird virtuelles Geld, aus einem realen Bankkonto wird ein virtuelles Bankkonto, aus einem realen Warenautomat wird ein virtueller Warenautomat und aus der realen Welt eine virtuelle Welt (oder viele virtuelle Welten). Durch die universell für die Verarbeitung digitaler Informationen einsetzbare digitale Hardware („Computer") kann jede digitale Information – gleich welchen Inhalts – beliebig verarbeitet, gespeichert und über digitale Infrastruktur übertragen werden. Und jede digitale Information kann als beliebiges „Irgendetwas" interpretiert, angezeigt, ausgegeben oder sonst wahrnehmbar gemacht werden. Wie es sich für virtuelle Sachverhalte gehört, sind diese nur innerhalb ihrer „Laufzeitumgebung" existent – so wie auch Gedanken in der Laufzeitumgebung unseres Gehirns (solange sie nicht außerhalb des Gehirns aufgezeichnet werden, z. B. in einem anderen Gehirn) oder Normen in der Laufzeitumgebung eines Rechtssystems existieren. Dieser Aspekt, dass ohnehin schon unsere halbe Welt immer „simuliert" war, indem die Bedeutung von Information nur innerhalb eines Bedeutungskontexts und einer spezifischen Laufzeitumgebung existiert, wird oft vernachlässigt. Virtuelle Welten sind nichts Neues – man

denke nur an philosophische Weltmodelle, antike Götterwelten, Steuervermeidungskonstruktionen oder das Datenschutzrecht. Es gab und gibt Menschen, die – abgesehen von Essen, Trinken und Schlafen – ausschließlich in solchen virtuellen Welten denken und leben.

Der Vorteil virtueller Welten ist, dass physikalische Gesetzmäßigkeiten wie Impulssatz, Thermodynamik oder Schwerkraft für sie nicht gelten. Manche drücken – einem Buch des US-amerikanischen Verfassungsrechtlers Lawrence Lessig von 1999 folgend – die Beziehung zwischen einer Simulations- bzw. Laufzeitumgebung, dem „code", und den damit „code-ifizierten" Rahmenbedingungen als „code as law" aus. In Wirklichkeit aber müsste es „code as reality" heißen. Denn der „code" simuliert erst einmal nur eine andere (virtuelle) Form von Realität, z. B. ohne Schwerkraft, oder dass man als Mitglied bei Facebook nun einmal in seinem Verhalten von vorne bis hinten observiert wird, ob man das nun will oder nicht. Es ist in der Facebook-Realität eine Art „Naturgesetz", natürlich von Facebook selbst so programmiert („code-ifiziert"), dass dies geschieht. Mit „law" hat das aber noch nichts zu tun. „law" beschreibt nicht, wie Laufzeitumgebungen (einschließlich der physikalischen Realität) oder deren Inhalte „sind", sondern, wie sie aufgrund der Vorgaben einer besonderen und einzigartigen Laufzeitumgebung, die sich „Rechtssystem" nennt, „sein sollen". Und gerade das Abweichen des Seins vom Sollen ist der Rechtsbruch. Der Satz „code breaches law" ist also nicht in sich widersprüchlich – was er wäre, wenn beides wie in „code as law" gleichgesetzt würde –, sondern gerade in Zeiten der DSGVO und der Anforderung „privacy by design" (Art. 25 Abs. 1 DSGVO) hoch aktuell.

Dabei wird auch deutlich, dass etwas, das „virtuell" oder „simuliert" ist, durchaus „real" sein kann – auch ein Computerspiel ist „real" in dem Sinne, dass man es „in der Realität spielt", und wer wegen Ketzerei verurteilt wurde, bekam zu spüren, wie „real" die Götter waren. Von daher war auch jede Gesellschaft immer schon eine „Informationsgesellschaft", weil Menschen (bzw. deren Gehirne) Informationen verarbeiten und Gesellschaften auf Informationsaustausch (bzw. Kommunikation) basieren. Das besondere an der digitalen Informationsgesellschaft ist nun, dass mit der Digitalisierung ein Weg – letztlich eine universelle Basissprache mit den Buchstaben 0 und 1 – gefunden wurde, Informationen nicht nur sehr unverlässlich zwischen Gehirnen (mündlich) oder wenig zugänglich über Schriftsprachen auszutauschen, sondern diese unverändert in Geräten zu speichern, zwischen Geräten hin- und herzutransferieren und den menschlichen Gehirnen praktisch überall wahrnehmbar machen zu können. Und diese Geräte werden immer größer und immer schneller.

Das nächste Problem ist es dann, gemeinsame (virtuelle) Sprachen zu finden, um die Insellösungen zu vernetzen, die es auch schon gibt, seit Menschen miteinander kommunizieren.

So, wie ein Mensch einer Stammessprache den Menschen einer anderen Stammessprache nicht versteht, so versteht auch eine Blockchain nicht die virtuellen Assets (Tokens) einer anderen Blockchain, so versteht auch Excel nicht SAP, so versteht auch ein MP3-Player kein HEVC / H.265. Das, was heute als „Industrie 4.0", als Blockchains, als Smart Contracts, als „Middleware" etc. bezeichnet wird, sind im Wesentlichen Standardisierungsbemühungen, also das Bestreben, mehr Systemen die gleiche (Meta-) Sprache und damit die gleichen Begriffsgerüste beizubringen, damit sie „vom selben reden". Und um das zu tun, werden täglich neue Begriffssysteme – Programmiersprachen, Datenstrukturen, Objektbeschreibungen, virtuelle offene oder geschlossene Umgebungen wie Facebook (für Kommunikation) oder Ethereum (für Smart Contracts) oder Rio (für Telematikdaten) etc. – erfunden, um Sprach- und damit Kommunikationsplattformen zu schaffen und so attraktiv zu gestalten, dass sie durch die „Sogwirkung der Marke" zu einer monopolartigen Universalplattform für alle werden. Smart Contracts etwa sind „nur" der Versuch, das, was die Juristen treffend „Vertragssprache" nennen, in eine (derzeit im Anfangsstadium ihrer Entwicklung befindliche) virtuelle Laufzeitumgebung zu „portieren", die als Ausführungsumgebung am besten dasselbe leisten soll wie die bisherige Ausführungsumgebung (also insbesondere die Gerichte), nur besser, schneller, vorhersehbarer und vernetzter mit angrenzenden Laufzeitumgebungen virtueller Systeme (wie Blockchains oder Smart Home-Netzen). Manchmal hat es aber den Anschein, als vergrößerten die vielen neuen und „gehypten" Insellösungen, die wie Unkraut aus dem Boden schießen, nur das babylonische Sprachgewirr. Entschuldigung, sprechen Sie Bitcoin Classic, Bitcoin Unlimited, Bitcoin XT oder Bitcoin ABC? Nein, ich spreche nur Bitcoin Cash und ein wenig Bitcoin Gold.

Was hat das alles mit der DSGVO zu tun? Das ist leicht erklärt. Unser Leben selbst transformiert sich in die digitale virtuelle Realität in dem Maße, in dem wir vor Bildschirm, Tastatur, Touchscreen, Maus, Stylus, Spracheingabesystem, Webcam etc. sitzen, also dort „leben". Deshalb produziert und hinterlässt auch jeder dort ständig immer mehr Informationen, im Begriffsjargon des Datenschutzes: personenbezogene Daten. Was früher noch eher der Umgang mit „personenbezogenen Sachen" war – meine Ziege, mein Haus, meine Münze, meine Lanze –, ist im Zeitalter der digitalvirtualisierten Gesellschaft der Umgang mit personenbezogenen Daten, die nun allgegenwärtig digital gespeichert, übermittelt und verwendet werden können. Dass virtuelle Laufzeitumgebungen stärker als davor die analoge Welt dazu neigen, jedes Detail der „Weltbewegung" als solches aufzuzeichnen und für immer zu speichern, ergab sich zunächst nur nebenbei durch die ewig sinkenden Speicherplatzpreise und die immer feinere Abtastung bei der Digitalisierung, hat aber mittlerweile ganz neue Möglichkeiten eröffnet („big data") und wird daher mit allen Mitteln forciert. Wenn dann auch noch alle Insellösungen miteinander sprechen (oder sogar dieselbe Sprache sprechen), wenn

also das Handelsregister mit dem Smart Contract und das Smart Home-Türschloss mit dem SAP-System redet, wenn alles immer digital und perfekt vernetzt ist, dann ist der (arme?) „Betroffene" nur noch das physische Anhängsel einer vollautomatischen Welt, in der ihn seine personenbezogenen Daten vollständig repräsentieren und letztlich ersetzen. Was früher das „mein" von „dein" abgrenzte – bestenfalls von „herrenlos" –, also das Sachenrecht, ist heute dasjenige, was die eigene „Betroffenheit" personenbezogener Daten von der Betroffenheit anderer, von Verantwortlichen und Auftragsverarbeitern – bestenfalls von anonymen Daten – abgrenzt: das Datenschutzrecht.

Man erkennt daran: Das Datenschutzrecht regelt nicht „nur mal eben so" den Schutz der Privatsphäre in Bezug auf personenbezogene Daten, die der böse Staat hat, um seine Bürger zu verwalten, oder die böse große Unternehmen haben, um noch mehr Konsum zu generieren und noch reicher zu werden, sondern es regelt alles. Jede Information, gleich ob Text, Bild, Video- oder Sprachaufnahme, Primärquelle oder Kommentierung; jede Speicherung, jede Verarbeitung, jede Übermittlung und Kommunikation; lediglich anonyme bzw. anonymisierte Daten und die Verarbeitung personenbezogener Daten „durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten" (Art. 2 Abs. 2 lit. c) DSGVO) sind ausgenommen. Wann aber Daten wirklich „anonymisiert genug" – also nicht mehr „rückbeziehbar" – sind, weiß niemand so genau. Und was wirklich noch im „Haushalt" bleibt, weiß auch niemand so genau. Das vermeintliche Regel-Ausnahme-Verhältnis („nur personenbezogene Daten sind Schutzgegenstand") ist in Wirklichkeit umgekehrt: Bei der weitaus überwiegenden Mehrzahl aller Daten gibt es „irgendeinen" Personenbezug, eben weil wir in einer Informationsgesellschaft leben, welcher der Personenbezug von Informationen wesensimmanent ist. In dieser Gesellschaft haben Daten ohne Personenbezug solange wenig Wert (oder sie haben doch einen Personenbezug), bis Maschinen intelligent genug sind, um sinn- und wertvolle Daten vollständig autonom zu generieren – und spätestens dann werden sie wohl auch von einem weiterentwickelten Datenschutzrecht als „betroffene Personen" erfasst werden. Der Begriff des „Personenbezugs" im Datenschutzrecht ist so ähnlich, als hätte man im Sachenrecht den „Atombezug" geregelt: Nur Sachen, die aus Atomen bestehen, sind vom Sachenrecht erfasst. Ach so! Na dann... Man hätte daher die DSGVO analog dem Sachenrecht auch „Informationsrechtsverordnung" nennen können. Und eben jene DSGVO verlangt nun von den „Verantwortlichen", gleich ob Unternehmen oder Privatpersonen (die häufig auch Verantwortliche sind), jedweden personenbezogenen Informationsschnipsel im weltweiten Informationsuniversum von der Wiege (insbesondere Erhebung) bis zur Bahre (Löschung) zu verfolgen („tracken") und darüber dem Subjekt der Information (dem Betroffenen) sowie den Aufsichtsbehörden zu jedem Zeitpunkt Rechenschaft abzulegen. Wer hat im Laufe der 26-jährigen beruflichen Karriere des Herrn Müller

bei der Firma Weber dessen Visitenkarte erhalten, was hat der Empfänger damit gemacht, wohin hat der Empfänger diese Kontaktinformationen weitergegeben, was hat der weitere Empfänger damit gemacht, in welchen CRM-Datenbanken befinden sich die Kontaktdaten jetzt etc.?

Eine derart epochale Verordnung, die direkt für über 500 Mio. Bürger und zusätzlich für eine unbekannte enorme Anzahl an Unternehmen, Behörden und sonstigen Institutionen – auch in Drittländern – Geltung entfaltet und beinahe jeden Umgang dieser Subjekte mit Information schlechthin regelt, müsste eigentlich mindestens so gut und lange durchdacht sein wie seinerzeit etwa das BGB. Zumal dann, wenn eine solche Verordnung jeden Verstoß mit Bußgeldern in Millionenhöhe sanktioniert. Der Gesetzestext lautet (Art. 83 DSGVO): „Bei Verstößen gegen die folgenden Bestimmungen werden [...] Geldbußen [...] verhängt". Das „werden" hieß nur in einer Vorversion der DSGVO noch „können". Lediglich bezüglich „Behörden und öffentlichen Stellen" kann der nationale Gesetzgeber entscheiden, „ob und in welchem Umfang" Geldbußen verhängt werden können (Art. 83 Abs. 7 DSGVO). Jedem, der sich nun darüber wundert, dass eine Weiterentwicklung des schon immer geltenden Datenschutzrechts solche Aufruhr verursacht, der sei noch einmal daran erinnert, dass die Datenschutzbehörden erst durch die DSGVO „Zähne bekommen haben", wobei sie dabei aber „nicht bissig geworden sind", wie es der hessische Datenschutzbeauftragte Michael Ronellenfitsch so niedlich ausdrückte. Was soll das heißen? Wenn man das Sachenrecht eingeführt hätte, ohne die Straftatbestände für Sachbeschädigung, Diebstahl, Untreue, Raub etc. einzuführen, wäre das Sachenrecht so belächelt worden wie ehemals das Datenschutzrecht. Die Unterscheidung zwischen „mein" und „dein" hätte nur auf dem Papier bestanden. Es hätte in 100 Jahren BGB nur eine Handvoll Urteile dazu gegeben, weil ein Wechsel von „mein" zu „dein" keine juristische Relevanz gehabt hätte. Vor diesem Hintergrund mutet es absurd an, einerseits die Vollzugsmöglichkeiten zu betonen („Zähne bekommen"), andererseits aber das Fortbestehen eines Vollzugsdefizits („nicht bissig") anzukündigen. Muss man sich nun daran halten oder nicht? Und wenn sich jemand nicht daran hält, gelten dann die Sanktionen der DSGVO oder nicht? Das klingt so, als sei man sich der Überregulierung (oder Überforderung?) bewusst, die sich bei wortlautgetreuer Auslegung der DSGVO an vielen Stellen ergibt, wollte aber dann doch nur das sanktionieren, was (nach welchen Maßstäben auch immer) „wirklich böse" ist.

Wer derart weitreichende Gesetze schreibt, sollte sich darüber bewusst sein, wie weitreichend sie sind, und sollte sie in möglichst allen Einzelheiten durchdacht haben, bevor er sie auf den Weg gibt. Dazu ist vor allem „Feldforschung" notwendig, also das Studieren dessen, was es „in der Realität" gibt. Für die DSGVO heißt das, sich darüber bewusst zu werden,

was personenbezogene Daten tatsächlich alles umfasst, welche Unternehmen, Kooperationen und „Betreibermehrheiten“ personenbezogene Daten wie nutzen und wofür sie sie in der Praxis benötigen bzw. verwenden. Dafür ist eine Menge detailliertes IT-Verständnis notwendig, denn die meisten personenbezogenen Daten einer Informationsgesellschaft werden mittlerweile in digitaler Form verarbeitet. Von diesem umfangreichen Wissen ausgehend kann man dann Fälle in Fallgruppen einteilen („clustern“) und Interessenabwägungen bzw. Wertungsentscheidungen vornehmen. Daneben kann man, so wie der Gesetzgeber des BGB über die grundsätzlich mit Sachen und Vertragstypen „machbaren“ Aktionen und Operationen nachgedacht hat, über die grundsätzlich mit digitalen Informationen „machbaren“ und mit virtuellen Objekten „simulierbaren“ Aktionen und Operationen nachsinnen und so zu einer universellen Begriffssprache und universellen Interessenausgleichsgrundsätzen und Wertungsvorgaben gelangen. Das Ganze kann man mehr oder weniger abstrakt regeln, um mehr oder weniger zukunftsoffen zu sein, wenn sich bestehende Modelle in Zukunft weiterentwickeln. Ein derartiges „bottom-up“-Vorgehen kann inklusive der vorangehenden „Feldforschung“ systematisch dokumentiert werden (zu Zeiten des BGB nannte man das die „Motive“) und gewinnt dadurch Überzeugungskraft, selbst wenn es nicht perfekt ist. Ein derart durchdacht konzipiertes Informationsrecht würde neben dem klassischen Datenschutzrecht auch das Urheberrecht, ein „Daten-Schadensersatzrecht“, vielleicht sogar ein „Daten-Eigentum“ und vielleicht noch vieles mehr umfassen, und so das große ganze System im Blick behalten, während es in Details heruntergebrochen wird. Im Gegensatz dazu macht die DSGVO den Eindruck, ihre Unkenntnis von ihrer eigenen Tragweite durch möglichst breitflächige bzw. abstrakte, phrasenhafte Formulierungen kaschieren zu wollen. So wird ein pseudo-präzises Begriffssystem, das in der Realität wenig Entsprechung findet, weil es nicht systematisch aus dieser abgeleitet, sondern „top-down“ entwickelt wurde, wie eine Käseglocke über die Informationsgesellschaft gestülpt und der Rest den Gerichten überlassen. Nichts kann dieses überstülpende „top-down“-Vorgehen besser dokumentieren als die hehren und ehrfurchtgebietenden Grundprinzipien, auf die sich die DSGVO selbst beruft (Art. 1 Abs. 1 DSGVO), die „Grundrechte und Grundfreiheiten natürlicher Personen“, von denen niemand weiß, welche genau dies eigentlich nun alles sein sollen. Politisch hingegen ist dieses Vorgehen durchaus verständlich: Einmal zu viel nachgedacht, ist die Legislaturperiode schon wieder zu Ende – also lieber (irgend-) etwas auf den Weg bringen als nichts.

Eine virtuelle Welt, in der Datenschutzverstöße unmöglich sind?

Das Thema Vollzug bzw. Vollzugsdefizit führt indes noch zu einem Gedanken, der im Zuge der Virtualisierung von allem und jedem immer populärer wird. Man kann virtuelle Systeme so ausgestalten, dass sie eine Rechtsordnung „automatisch" umsetzen. Neudeutsch nennt sich das „embedded law". Ein vom Gesetzgeber in Form von Normen vorgegebenes Rechtsverständnis wird Teil der Struktur des virtuellen Systems. Man kann ein Computerspiel so programmieren, dass alles, was in der realen Welt möglich ist, auch in der Simulation möglich ist, außer wenn dabei Gesetze gebrochen werden. Möchte ein Spieler einen anderen Spieler umbringen und ihm dazu ein Messer in den Rücken stechen, dann geht das nicht. Vielleicht erweist sich der Rücken des anderen Spielers als hart wie Stein oder das Messer verschwindet einfach, aber das Erstechen ist nicht möglich, weil das Computerspiel diese Möglichkeit nicht vorsieht. Oder man kann ein Auto erst starten, wenn man vorher einen Alkoholtest bestanden hat. Sonst fährt das Auto nicht los, weil das System das nicht erlaubt. Man könnte dies „Vollzug aus sich selbst heraus" nennen – ein System vollzieht rechtliche Vorgaben ohne (An-) Klage, ohne Gericht, ohne Gerichtsvollzieher, Gefängnis, Zwangshypothek, so wie sich physikalische Gesetze selbst vollziehen. Ein System kann übrigens auch so gestaltet sein, dass es Recht verletzt, wie eine Software, deren Zweck das „Knacken" eines Kopierschutzes ist. Aber vielleicht verletzt es Recht nur in einem Staat und nicht in einem anderen, oder es verletzt Recht nur, wenn man die herrschende juristische (Auslegungs-) Meinung zugrunde legt (und nicht „eine im Vordringen befindliche Mindermeinung", wie man so schön sagt).

„Compliance" ist die Vorgabe, das (virtuelle) System eines Unternehmens möglichst so zu gestalten, dass Rechtsverstöße „so gut wie nicht" passieren können. Das können organisatorische Vorgaben an Menschen oder technische Vorgaben an Maschinen sein. Noch besser wäre es natürlich, wenn die Beschaffenheit eines virtuellen Systems von vornherein so angelegt werden könnte, dass Verstöße nicht möglich sind, so sehr man sich auch anstrengen mag. Die DSVGO gibt ein klares Compliance-Ziel vor: Der Verantwortliche und der Auftragsverarbeiter sollen Systeme und Kontrollen einführen und alles dokumentieren, um sicherstellen und beweisen zu können, dass die DSGVO jederzeit und von allen unterstellten Personen eingehalten wurde. Im Bereich der Vorgaben für die Beschaffenheit technischer Maßnahmen bleibt die DSGVO notwendigerweise halbherzig – unter sehr schwammig formulierten Voraussetzungen („Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbei-

tung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen“) soll der Verantwortliche u. a. die Hard- und Software so auslegen, dass sie in der Lage ist, „die Datenschutzgrundsätze [...] wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen“ (Art. 25 Abs. 1 DSGVO). Wenn man das etwas konsequenter liest als es hier wohl gemeint ist, muss die digitalvirtualisierte Welt so strukturiert werden, dass Datenschutzverstöße schlicht nicht möglich sind. Die zweckfremde Nutzung personenbezogener Daten, die widerrechtliche Nicht-Löschung, die unterlassene Pflichtinformation gegenüber dem Betroffenen – das setzt dann nicht mehr die Frage voraus, ob man sich rechtstreu verhalten „will“, sondern man „kann“ sich nur rechtstreu verhalten oder gar nicht.

Wie wird das umgesetzt? Ganz einfach. Man muss nur sämtliche personenbezogenen Daten (also eigentlich alle Daten?) in einem Berechtigungssystem kapseln, also „einschließen“, und nur derjenige bekommt solange Zugriff auf die Daten, wenn und solange er eine legitime Nutzung nachweisen kann – und natürlich wird jede Nutzungshandlung in Echtzeit daraufhin kontrolliert, ob sie mit der ursprünglich angemeldeten und für legitim befundenen Nutzungsabsicht in Einklang steht. Jedes von einem Verantwortlichen neu erhobene personenbezogene Datum wandert also sofort in einen „Datensafe“ und wird ab dann nur noch durch einen universellen Link darauf ersetzt. Man spricht ja auch im Internet so treffend vom „Uniform Resource Locator“ (URL). Eine Information, etwa ein Dokument, die das personenbezogene Datum enthält, enthält also nur die URL des personenbezogenen Datums. Möchte jemand das Datum selbst „sehen“ (bzw. nutzen), muss er sich und seine datenschutzrechtliche Berechtigung gegenüber dem Datensafe ausweisen. Er erhält dann Zugriff auf das personenbezogene Datum, natürlich in einer solchen Form und innerhalb eines solchen Zeitraums, dass damit keine andere Nutzung möglich ist als diejenige, welche die DSGVO vorsieht. Im Datensafe wird alles unveränderbar protokolliert, bei Löschung des ursprünglichen personenbezogenen Datums wird der Datensatz verschlüsselt, archiviert und der Schlüssel an eine „trusted third party“ übertragen, um später nachweisen zu können, dass alles „mit rechten Dingen“ zugegangen ist. Datenübermittlung an Dritte? Nicht möglich, nur die URL kann weitergegeben werden. Daten einfach nicht löschen? Keine Chance, irgendwann geht der Zugriff auf die URL ins Leere. Umgehung durch Abfotografieren des Bildschirms? Versuchen Sie es mal; Ihr Smartphone wird dieses Foto ebensowenig aufnehmen wie Ihr Farbkopierer Geldscheine kopiert. Werbung an die Person verschicken ohne datenschutzrechtliche Legitimationsgrundlage? Die Werbe-E-Mail bleibt in Ihrem Server hängen.

Eine solche pointierte Vision des „totalen Vollzugs aus sich selbst heraus“ mag erschreckend erscheinen, aber eigentlich war es doch immer der selbstverständliche Anspruch des Rechts in einem Rechtsstaat, dass es zu einhundert Prozent eingehalten wird. Nur die Beschränkungen der physikalischen Welt haben das verhindert – oder nur das Recht „akzeptabel“ werden lassen? Die digitalvirtualisierte Welt kann es ermöglichen, dass Autos keine Geschwindigkeitsüberschreitungen mehr ausführen können, dass nichtzahlende Mieter ihre Wohnungen nicht mehr betreten können, dass man mit einem 3D-Drucker keine Waffen ausdrucken kann – warum also nicht auch der vollautomatische, totale Datenschutz ohne Aufsichtsbehörden und Gerichte. Wenn es um Mord und Totschlag ginge, wäre wohl jeder sofort dabei – wie schön, wenn es das nicht mehr geben würde, weil es niemand mehr verüben *könnte*. Hört beim Datenschutzverstoß der Spaß auf? Wenn das alle so sähen, wäre wohl irgendwas faul an der DSGVO.

„Schön, dass wir mal so offen über alles gesprochen haben!“

So bewegen sich am Ende dieses Exkurses die einzelnen Elemente aufeinander zu. Die DSGVO hat zwar einen universellen Geltungsanspruch, ist aber viel zu unbestimmt, als dass sie automatisiert werden könnte. Wer sich nur beispielsweise einmal Gedanken zum Verhältnis der DIN 66398 für Löschkonzepte zur DSGVO gemacht und Löschklassen, Datenarten und Löschregeln in dreistelliger Anzahl gebildet hat, der wird erkennen, dass – wie es Juristen gerne tun – die Komplexität schon in mittelgroßen Unternehmen beliebig gesteigert werden kann. Das Ergebnis erscheint einem durchschnittlichen Unternehmer absurd und monströs; Sabotage im Alltag ist vorprogrammiert. Liegt das an der DSGVO oder an der störrischen menschlichen Natur? „Die Geister, die ich rief, werd‘ ich nun nicht mehr los“: Die zunehmende Komplexität des Rechts folgt der zunehmenden Komplexität der Realität, was es schwierig macht, diese sich in der DSGVO als große Unbestimmtheit niederschlagende Komplexitätszunahme in deterministische Prozess- und Programmabläufe zu packen. Obwohl doch diese unternehmensinterne Implementation automatisierter und automatisch datenschutzrechtskonformer Prozesse eigentlich genau das ist, was sich der Gesetzgeber vorstellt und den Rechtsanwendern in einer „light“-Version als „technische und organisatorische Maßnahmen“ ins Stammbuch schreibt. Aber je unbestimmter das Gesetz, desto mehr juristische Prüfungsarbeit, desto mehr Grübeln über „die besonderen Umstände des Einzelfalls“ ist notwendig. Das Datenschutzrecht, das wie ein „Layer“ auf die tägliche Arbeit insbesondere in Unternehmen gestülpt wird, erfordert daher noch eine Menge Arbeit von jener Disziplin, die sich seit den 1970er-Jahren mit bislang mäßigem Erfolg mit der Formalisierung und Automatisierung von Recht beschäftigt – der Rechtsinformatik. Leider können dazu bis-

lang weder das Einspeisen von Millionen von Gerichtsentscheidungen (die es im Datenschutzrecht gar nicht gibt) und die vermeintlich „künstlich intelligente“, letztlich aber „nur“ großdimensional statistische Mustersuche in diesen Quellen noch die grob vereinfachenden Prototypen-Apps der „Legal Hackathons“ aus den Programmbibliotheken-Baukästen einen sinnvollen Beitrag leisten. Bis zur Verfügbarkeit funktionierender, tatsächlich „disruptiver“ Automatisierungslösungen droht das Datenschutzrecht von der Mehrheit der Gesetzesadressaten, die glücklich hinter den (datenschutzrechtlichen) Wäldern hausen, weiter weitgehend ignoriert zu werden.

Experten-Kontakt

Dr. Axel-Michael Wagner
Rechtsanwalt

E-Mail: a.wagner@psp.eu

Über PSP

Peters, Schönberger & Partner (PSP) zählt mit einer 40-jährigen, erfolgreichen Unternehmenshistorie zu den renommiertesten mittelständischen Kanzleien in Deutschland. Als Steuerberater, Wirtschaftsprüfer und Rechtsanwälte unterstützen wir Sie bei wichtigen Entscheidungen und begleiten Sie bei deren Umsetzung. Zu unseren Mandanten zählen mittelständische Unternehmen, Familienunternehmen, vermögende Privatpersonen und Private Equity-Gesellschaften, die den Wunsch nach einer interdisziplinären und individuellen Beratung haben. Sie finden in uns einen professionellen, verlässlichen und durchsetzungsstarken Partner, der mit Leidenschaft Ihre rechtlichen und steuerlichen Interessen vertritt und auch die klassischen Aufgaben der Wirtschaftsprüfer übernimmt. Das PSP-Family Office unterstützt Sie zudem bei der Vermögensstrukturierung und verfügt über ausgewiesene Expertise in Nachfolge-, Stiftungs- und Immobilienfragen.

PETERS, SCHÖNBERGER & PARTNER
RECHTSANWÄLTE
WIRTSCHAFTSPRÜFER
STEUERBERATER
www.psp.eu