

## **Wann darf man Daten verarbeiten?**

Die Rechtsgrundlagen in Art. 6 Abs. 1 DSGVO und in § 26 Abs. 1 BDSG-neu

*Auf einen Menschen bezogene Daten sind keine Sachen, die allen gehören. Über andere Informationen zu sammeln, sie zu speichern und bei Gelegenheit auszuwerten, ist grundsätzlich verboten. Eine Ausnahme gilt im rein familiären Bereich sowie dann, wenn das geltende Recht eine ausdrückliche Erlaubnis gewährt. An diesem „Verbot mit Erlaubnisvorbehalt“ hat auch die DSGVO nichts geändert. Die konkreten Grenzen zwischen „erlaubt“ und „verboten“ haben sich jedoch ein wenig verschoben; sie werden hier im Einzelnen dargestellt.*

von **Wolfgang Däubler**

Nehmen wir zunächst den Fall eines Facebook-Nutzers. Alles, was er bei Facebook macht, seine Postings, die Auswahl seiner „Freunde“, aber auch sein Profil werden automatisch in die USA übermittelt. Was dort mit diesen Daten geschieht, ist schwer herauszubekommen. Kann er sich in einer solchen Situation auf die DSGVO berufen und z. B. nach deren Art. 15 einen Auskunftsanspruch gegen Facebook/USA geltend machen?

### **Datenschutz auch gegenüber US-Unternehmen?**

Nach bisherigem Recht war dies zumindest schwierig, weil das deutsche BDSG nur auf Verarbeitungen anwendbar war, die im Inland stattfanden. Ab 25. Mai 2018 gilt jedoch Art. 3 DSGVO, und danach kann sich unser User auf das europäische Datenschutzrecht berufen. Dieses findet nach Art. 3 Abs. 1 Anwendung, wenn ein Unternehmen aus einem Drittstaat eine Niederlassung in der EU hat, was bei Facebook ja der Fall ist. Die Übermittlung in die USA ist also nur dann erlaubt, wenn sie die DSGVO zulässt. Insoweit müssen besondere Voraussetzungen erfüllt sein, auf die im Rahmen eines anderen Beitrags einzugehen ist.<sup>1</sup>

Aber wie verhält es sich, wenn Facebook/USA die Daten direkt erhebt und seine europäische Niederlassung gar nichts damit zu tun hat? Facebook bietet vielfältige „Dienste“ an und deshalb ist Art. 3 Abs. 2 Buchstabe a DSGVO anwendbar: Unternehmen aus Drittstaaten, die in der EU Waren oder Dienstleistungen anbieten, unterliegen dabei dem europäischen

---

<sup>1</sup> Wedde

Datenschutzrecht. Sie müssen also z. B. Auskunft geben, welche Daten sie gespeichert haben und was sie mit ihnen anfangen wollen.

Doch wer wird in Texas oder Kalifornien eine Klage auf Auskunft erheben? Abenteurer dieser Art sind höchst seltene Exemplare. Und was geschieht, wenn die Aufsichtsbehörde einen mahnenden Brief schreibt, aber aus den USA keine Antwort kommt? An solche Fälle hat der europäische Gesetzgeber durchaus gedacht: Art. 27 DSGVO verlangt, dass Unternehmen aus Drittstaaten in der EU einen Vertreter bestellen, an den sich die Betroffenen ebenso wie auch die Aufsichtsbehörden wenden können. Tun die Unternehmen das nicht, kann die Aufsichtsbehörde „geeignete Maßnahmen“ ergreifen. Nach Art. 58 Abs. 2 Buchstabe f DSGVO darf sie u. a. die Datenverarbeitung durch das Unternehmen beschränken und im Extremfall sogar verbieten. Sie kann dieses also letztlich vom Markt vertreiben, wenn es die hier herrschenden Regeln nicht einhält. Auch das gab es bisher so noch nicht. Ob es dann wirklich passiert, ist eine andere Frage, aber die rechtlichen Möglichkeiten sind eröffnet.

Man kann das alles mit der Formel zusammenfassen, dass die DSGVO immer anwendbar ist, wenn Menschen in der EU betroffen sind. Ähnlich verfährt auch das US-Recht, wenn es um den Schutz Minderjähriger im Internet geht: Hier müssen die europäischen Firmen das US-Recht beachten, wenn sie von hier aus Angebote machen. Wir können also im Folgenden davon ausgehen, dass die DSGVO auch bei Auslandskontakten Anwendung findet, die ja immer häufiger werden.

### **Die Ermächtigungen nach Art. 6 DSGVO**

Wann ist nun Datenverarbeitung (ausnahmsweise) erlaubt? Die ansonsten nicht immer leicht zu lesende DSGVO kommt uns hier entgegen: Die „Ermächtigungstatbestände“ sind in Art. 6 Abs. 1 im Einzelnen aufgezählt. Die DSGVO benutzt dabei einen weiten Begriff von Datenverarbeitung, der auch die Erhebung, die Nutzung und die Löschung, also letztlich jede Form des Umgangs mit Daten erfasst. In Art. 6 Abs. 1 sind insgesamt sechs Fallkonstellationen aufgeführt, von denen drei die bei weitem größte praktische Bedeutung haben: Die Einwilligung (Buchstabe a), die Anbahnung und Durchführung eines Vertrages (Buchstabe b) und die Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen oder Grundrechte der betroffenen Person überwiegen (Buchstabe f). Die drei anderen Fälle darf man nicht übersehen, aber sie sind von geringerer

Bedeutung: Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich (Buchstabe c), was etwa bei der Übermittlung von Arbeitnehmerdaten an die Sozialversicherungsträger und an die Finanzbehörden der Fall ist. Die Verarbeitung ist notwendig, um lebenswichtige Interessen einer Person zu schützen (Buchstabe d), was z. B. bei der Ermittlung der Blutgruppe eines bewusstlosen Unfallopfers anzunehmen ist, das dringend eine Bluttransfusion benötigt. Schließlich geht es darum, dass die Datenverarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder bei der der Verantwortliche hoheitlich handelt, weil ihm entsprechende Befugnisse übertragen wurden (Buchstabe e). Eine Bank ist etwa verpflichtet, zur Verhinderung von Geldwäsche bestimmte Daten zu erheben und an die Aufsichtsbehörde weiterzugeben. Das soll uns hier nicht weiter interessieren. Im Folgenden werden die drei wesentlichen Fälle geschildert.

### **Datenverarbeitung kraft Einwilligung**

Die Einwilligung ist auf der einen Seite Ausdruck der informationellen Selbstbestimmung: Die betroffene Person befindet selbst darüber, was mit ihren Daten geschieht, wer in welcher Weise mit ihnen umgehen darf.<sup>2</sup> Auf der anderen Seite steht diese Freiheit auf dem Papier, wenn jemand auf ein Bankkonto, einen Strom- und einen Telefonanschluss oder eine Versicherung angewiesen ist: Hier geht seine Freiheit gegen null, wenn die andere Seite eine „Einwilligung“ in die Preisgabe von Daten verlangt. Er wird das tun, was ihm nahe gelegt wird. Die Freiheit wird zur Unterwerfung.

Auch ohne eine solche Zwangslage bestehen Gefahren. Es kann zu einer umfassenden Kommerzialisierung höchstpersönlicher Daten kommen, die z. B. in sozialen Medien „abgeschöpft“ werden. Das Privatleben, die persönlichen Präferenzen für bestimmte Bücher, für eine spezifische Art Musik, aber auch für die Einnahme bestimmter Medikamente wird erfasst und – so die harmloseste Konsequenz – für möglichst geschickt ausgesuchte künftige Angebote verwendet. Die Vermarktung erobert Lebensbereiche, die ihr aus grundsätzlichen Erwägungen verschlossen bleiben sollten.<sup>3</sup>

---

<sup>2</sup> Fladung/Pötters, in: Wybitil (Hrsg.), EU-Datenschutz-Grundverordnung, 2017, Art. 7 Rn. 3.

<sup>3</sup> Zu den rechtlichen Grenzen der Kommerzialisierung s. den Überblick bei Däubler, BGB kompakt, 3. Aufl. 2008, Kap. 6.

Die Regelungen in der DSGVO und in § 26 Abs. 2 BDSG-neu wollen diesen Entwicklungen entgegenwirken. Sie lassen eine wirksame Einwilligung nur dann zu, wenn bestimmte Voraussetzungen erfüllt sind.

(1) Die betroffene Person muss wissen, um was es geht. Sie muss die nötige Einsichtsfähigkeit besitzen, um die Tragweite der Einwilligung beurteilen zu können. Dies ist besonders deshalb wichtig, weil nach Art. 8 DSGVO Minderjährige bereits mit 16 Jahren „netzmündig“ sind, also im Internet ohne Einschaltung ihrer Eltern eine Einwilligung erteilen können. Notwendig ist aber nicht nur für diese Gruppe, sondern für alle Einwilligenden eine umfassende Aufklärung über die beabsichtigte Verwendung und die damit unter Umständen verbundenen Risiken. Dabei muss präzise angegeben werden, für welche Zwecke die Daten verwendet und an wen sie ggf. übermittelt werden. Pauschale Hinweise („gute Zwecke“ oder „Verwendung im Rahmen der geschäftlichen Interessen des Unternehmens“) genügen nicht.

(2) Nach bisherigem Recht (§ 4a Abs. 1 Satz 3 BDSG-alt) bedurfte die Einwilligung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen war. Dahinter stand der Gedanke des Übereilungsschutzes: Bevor man eine Unterschrift leistet, denkt man eher als bei einem Click darüber nach, ob man das wirklich machen soll oder nicht. Die DSGVO hat diese Regelung nicht übernommen. Vielmehr muss es sich bei der Einwilligung lediglich um eine »unmissverständlich abgegebene Willensbekundung« (Art. 4 Nr. 11) handeln, die auch mündlich oder konkludent erfolgen kann.<sup>4</sup> Allerdings muss die „Willensbekundung“ in einem aktiven Tun bestehen; Stillschweigen oder Untätigkeit genügen nicht. Für das Beschäftigungsverhältnis hält § 26 Abs. 2 BDSG-neu jedoch an der bisherigen Schriftform fest.

(3) Schon nach altem Recht durfte die Einwilligung keinen pauschalen Charakter haben. Vielmehr musste sie erkennen lassen, welche Daten zu welchem Zweck verarbeitet oder genutzt werden sollten.<sup>5</sup> Dies bringt Art. 4 Nr. 11 DSGVO in der Weise zum Ausdruck, dass die Einwilligung »für den bestimmten Fall« erteilt werden muss. Dabei können mehrere Zwecke verfolgt werden (wie Art. 6 Abs. 1 Buchst. a DSGVO deutlich macht), doch müssen sie klar zum Ausdruck gebracht sein und dem Betroffenen die Auswahl lassen, auch einzelne Zwecke abzulehnen.<sup>6</sup> Das rechtfertigt sich damit, dass nur auf diese Weise der Vorgang für

---

<sup>4</sup> „Konkludent“ meint, dass andere aus dem Umständen wie Kopfnicken oder Entgegennahme einer Ware schließen können, dass eine bestimmte Erklärung gewollt ist.

<sup>5</sup> S. statt aller Klug, RDV 2001, 272; Wohlgemuth, BB 1996, 693.

<sup>6</sup> Klabunde, in: Ehmann/Selmayr, Kommentar zur DSGVO, 2017, Art. 4 Rn. 36.

den Einzelnen überschaubar und damit transparent bleibt. Auch derjenige, der sich über die Bedeutung seines Tuns voll bewusst ist, kann daher nicht in eine „Verwendung nach Belieben“ oder „für Zwecke einer Verbesserung der Arbeitsabläufe“ einwilligen.

(4) Die Einwilligung darf nicht gegen zwingendes Recht verstoßen. So darf etwa das Fragerecht des Arbeitgebers gegenüber Bewerbern nicht durch Einwilligung erweitert werden, und die Einwilligung darf auch keine unbillige Benachteiligung der betroffenen Person im Sinne des § 307 Abs. 1 BGB darstellen.

(5) Die Einwilligung muss schließlich „freiwillig“ sein, was schon die Definition in Art. 4 Nr. 11 DSGVO zum Ausdruck bringt. Der Einwilligende darf nicht in unangemessener Weise unter Druck gesetzt werden. Dafür würde es schon genügen, ihm in Aussicht zu stellen, dass seine Anliegen in Zukunft „mit weniger Entgegenkommen als bisher“ geprüft würden. Auch lässt Art. 7 Abs. 4 DSGVO die Freiwilligkeit dann entfallen, wenn bei Vertragsverhandlungen von der betroffenen Person Daten abverlangt werden, die für die Durchführung des Vertrages nicht erforderlich sind. Wer ein Smartphone kauft, soll seine Daten auch „für Werbezwecke“ zur Verfügung stellen; genau das geht nicht mehr.

### **Das Sonderproblem: Einwilligung durch Beschäftigte**

Besonders problematisch ist die Freiwilligkeit im Arbeitsverhältnis. Der deutsche Gesetzgeber hat sich dieses Problems (ein wenig) angenommen und in § 26 Abs. 2 Satz 1 und 2 BDSG-neu zwei allgemeine Grundsätze festgelegt. Nach Satz 1 muss bei der Beurteilung der Freiwilligkeit neben den konkreten Umständen die „Abhängigkeit“ berücksichtigt werden, die im Beschäftigungsverhältnis besteht. Konkreter wird Satz 2: Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder wenn Arbeitgeber und Arbeitnehmer gleichgerichtete Interessen verfolgen. Daraus wird man schließen können, dass immer dann, wenn die Einwilligung dem Beschäftigten lediglich Nachteile bringt, nicht von Freiwilligkeit die Rede sein kann.<sup>7</sup> Dies alles wird an Beispielen deutlich.

Ist die Weitergabe von Daten an ein anderes Konzernunternehmen Voraussetzung für eine konzernweite Sonderleistung wie z. B. eine Aktienoption, so ist im Regelfall von

---

<sup>7</sup> So zutreffend Wybitul, NZA 2017, 413, 416.

Freiwilligkeit auszugehen. Dasselbe gilt dann, wenn der Beschäftigte den Wunsch äußert, dass seine Bewerbungsunterlagen für den Fall, dass er die erstrebte Stelle nicht erhält, an ein anderes Konzernunternehmen weitergegeben werden. Weitere Beispiele sind die Teilnahme an einem betrieblichen Gesundheitsmanagement und die Erlaubnis, die betrieblichen Telekommunikationseinrichtungen auch für private Zwecke zu verwenden.<sup>8</sup> Gleichgerichtete Interessen sind dann anzunehmen, wenn ein Werbefilm über die Arbeit im Betrieb gedreht wird und sich Beschäftigte auf eigene Initiative daran beteiligen können.<sup>9</sup>

Umgekehrt wäre eine Erklärung des Beschäftigten, der Arbeitgeber könne jederzeit seinen privaten Spind kontrollieren, im Regelfall unfreiwillig und deshalb im Ergebnis unwirksam.<sup>10</sup> Erst recht gilt dies, wenn der Arbeitgeber Nachteile androht. Das BAG nimmt in einem solchen Fall schon nach bisherigem Recht einen „groben Verstoß gegen die arbeitgeberseitigen Pflichten aus § 241 Abs. 2 BGB und § 612a BGB“ an.<sup>11</sup> Die Freiwilligkeit ist auch dann aufgehoben, wenn der Arbeitnehmer davon ausgeht, ihm könnten bei einer Verweigerung Nachteile drohen, sofern diese Befürchtung nicht völlig aus der Luft gegriffen ist.

Geht es um eine generelle Regelung im Betrieb, so greifen Arbeitgeber nur selten auf das Mittel „Einwilligung“ zurück: Aus ihrer Sicht besteht immer das Risiko, dass im Streitfall ein Gericht die „Freiwilligkeit“ verneint. Auch könnten einzelne Arbeitnehmer von ihrem Widerrufsrecht Gebrauch machen, das sie schon bisher hatten, das ihnen jetzt aber Art. 7 Abs. 3 DSGVO ausdrücklich gewährt.

## **Abschluss und Durchführung von Verträgen**

Der zweite wichtige Erlaubnistatbestand ist der Vertrag d. h. sein Abschluss, seine Durchführung und am Ende seine Abwicklung. Daten, die dafür notwendig sind, dürfen nach Art. 6 Abs. 1 Buchstabe b DSGVO erhoben und verarbeitet werden.

Verträge können einen ganz unterschiedlichen Charakter haben. Wer in einer fremden Stadt drei Brötchen kauft und sofort bezahlt, hat einen Vertrag geschlossen, bei dem personenbezogene Daten ersichtlich keine Rolle spielen. Wer von einer Bank ein Darlehen für

<sup>8</sup> Beide Beispiele bei Gola, BB 2017, 1462, 1467.

<sup>9</sup> S. den ähnlichen Fall BAG 11.12.2014 – 8 AZR 1010/13, NZA 2015, 604.

<sup>10</sup> S. den Sachverhalt in BAG 20.6.2013 – 2 AZR 546/12, ZD 2014, 260.

<sup>11</sup> BAG 11.12.2014 – 8 AZR 1010/13, NZA 2015, 604, 607 Tz. 32.

den Hauskauf haben will, muss seine Einkommens- und Vermögensverhältnisse bis ins Detail darlegen und ggf. in eine Schufa-Auskunft einwilligen – die Bank will sicher sein, dass sie ihr Geld wiederbekommt. Zwischen diesen beiden Extremen liegt der Mietvertrag über eine Wohnung – der Vermieter kann eine Verdienstbescheinigung verlangen (aus der der Arbeitgeber und der Monatsverdienst deutlich wird), aber nicht danach fragen, ob in der Vergangenheit Schulden immer pünktlich beglichen wurden.

Auch der Arbeitsvertrag fällt unter Art. 6 Abs. 1 Buchstabe b DSGVO, doch hat der deutsche Gesetzgeber auf der Grundlage der Öffnungsklausel des Art. 88 Abs. 1 DSGVO in § 26 Abs. 1 Satz 1 BDSG-neu eine Sonderregelung geschaffen. Danach dürfen Daten von Beschäftigten verarbeitet werden, wenn dies für die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist. Damit ist ein weiterer Bereich eröffnet, aber zugleich sind zwei wesentliche Schranken deutlich gemacht.

Zum einen muss ein Bezug zum Beschäftigungsverhältnis gegeben sein. Geht es um andere Zwecke wie z. B. die Gestaltung des Privatlebens, kann sich der Arbeitgeber nicht auf § 26 Abs. 1 Satz 1 BDSG-neu stützen, wenn er beispielsweise wissen will, ob jemand in der Freizeit Sport treibt oder gerne zur Zigarette greift.

Zum zweiten müssen die angefragten oder auf anderem Wege ermittelten Daten für die Beschäftigung „notwendig“ sein; bloße Nützlichkeit oder „Dienlichkeit“ genügt nicht. So kann es zwar für einen Personalleiter von Interesse sein, Näheres über das Familienleben des Beschäftigten zu erfahren, weil dies auch das Verhalten im Betrieb (positiv oder negativ) beeinflussen kann, doch sind solche Informationen im Regelfall für die Durchführung des Arbeitsverhältnisses nicht „erforderlich“.

In der Praxis gibt es viele Zweifelsfragen. Ist es beispielsweise zulässig, über einen eingebauten GPS-Sensor jederzeit den Ort feststellen zu können, wo sich der Fahrer oder der Außendienstmitarbeiter gerade befindet? Ist der Arbeitgeber ein Transportunternehmer, wird er vielleicht ein „Flottenmanagement“ begrüßen, das ein „Umdirigieren“ einzelner Fahrer ermöglicht, um schnell auf Kundenerwartungen reagieren zu können. Macht dies den GPS-Einsatz notwendig oder würde es auch genügen, wenn jeder Fahrer auf Handy erreichbar ist? Ist in einer Forschungsabteilung eine Zugangskontrolle durch Fingerabdrücke geboten oder genügt ein Werksausweis mit Foto? Soweit ein Betriebsrat besteht, hat dieser ein

Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG, weshalb es meist nicht bei der „Grauzone“ bleibt sondern ein klare, datenschutzfreundliche Lösung geschaffen wird. In anderen Fällen kommt es allein auf die datenschutzrechtliche Situation an, wobei es noch immer relativ wenig Rechtsprechung gibt, die weiterhelfen könnte.

### **Ermittlungen in Verdachtsfällen**

Sehr viel größere Spielräume hat der Arbeitgeber, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat (§ 26 Abs. 1 Satz 2 BDSG-neu). Die „Anhaltspunkte“ sind vom Arbeitgeber zu dokumentieren. In einem solchen Fall kann sogar eine heimliche Videoüberwachung<sup>12</sup> und der verdeckte Einsatz von Privatdetektiven<sup>13</sup> zulässig sein, wenn keine weniger eingreifenden, „milderen“ Mittel zur Verfügung stehen. Genauso wird von der Rechtsprechung verfahren, wenn der Verdacht einer schweren Verletzung arbeitsvertraglicher Pflichten besteht, wobei unmittelbar auf § 26 Abs. 1 Satz 1 BDSG-neu zurückgegriffen wird.<sup>14</sup> Dagegen bestehen zahlreiche Einwände, doch können sie schon aus Raumgründen hier nicht dargestellt werden.<sup>15</sup> Zusätzliche Bedenken ergeben sich dadurch, dass Art. 6 Abs. 1 DSGVO Fälle dieser Art nicht erwähnt, da der Arbeitgeber kein Strafverfolgungsorgan ist; Art. 88 Abs. 1 DSGVO ermächtigt jedoch nur zu „spezifischeren“, nicht zu andersartigen Vorschriften.

### **Überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten**

Der Rückgriff auf Art. 6 Abs. 1 Buchstabe f DSGVO kann für den Arbeitgeber verführerisch sein, um sich so den arbeitsrechtlichen Vorgaben zu entziehen. Zunächst zu den Voraussetzungen der Vorschrift.

Der Verantwortliche muss ein „berechtigtes Interesse“ an der Erhebung oder Verarbeitung von Daten haben. Er will beispielsweise einen Betrieb oder gar das ganze Unternehmen verkaufen und bei dieser Gelegenheit die Qualifikation bestimmter Mitarbeiter in den Vordergrund stellen. Auch ein Kaufinteressent wird als Dritter solche Informationen begrüßen, ja sogar verlangen, da sie für die Einschätzung der Zukunftsaussichten recht hilfreich sind. Dass bei beiden ein berechtigtes Interesse vorliegt, wird man schwerlich

---

<sup>12</sup> BAG NZA 2008, 1187

<sup>13</sup> BAG NZA 2017, 1179; kritisch dazu Däubler, NZA 2017, 1481, 1485.

<sup>14</sup> BAG NZA 2017, 1327.

<sup>15</sup> Nachweise bei Däubler, Gläserne Belegschaften, 7. Aufl. 2017, Rn. 379 ff.

bestreiten können, doch überwiegt es auch gegenüber den Interessen und Grundrechten der betroffenen Arbeitnehmer? Wer sich auf der „Leistungssträgerliste“ befindet, ist in seinem informationellen Selbstbestimmungsrecht nur wenig berührt; für eine solche Heraushebung bedarf es nicht unbedingt seiner Einwilligung. Wie steht es aber mit denjenigen, die sich nicht auf der Liste wiederfinden? Unterstellt, das Unternehmen wird tatsächlich verkauft, so kann es die weitere Laufbahn erheblich beeinträchtigen, wenn X oder Y nur als „durchschnittlich“ eingestuft wurden. Hier ist der Vorrang der Arbeitgeber- und Käuferinteressen keineswegs evident.

Bevor man hier Farbe bekennt, muss allerdings Klarheit darüber bestehen, ob und inwieweit Art. 6 Abs. 1 Buchstabe f überhaupt neben vertraglichen Beziehungen Anwendung finden kann. Soweit es um die Durchführung des Beschäftigungsverhältnisses geht, ist nur ein Rückgriff auf Art. 6 Abs. 1 Buchstabe b bzw. § 26 Abs. 1 BDSG-neu möglich: Der Arbeits- oder Beschäftigungsvertrag legt für den Bereich „Beschäftigung“ verbindlich den Verarbeitungsrahmen fest, in den die Interessen beider Seiten eingehen. Wollte man Buchstabe f daneben anwenden, könnten die vertraglichen Abmachungen überspielt und nachträglich durch andere Ergebnisse ersetzt werden. Das bedeutet, dass Art. 6 Abs. 1 Buchstabe f nur dann herangezogen werden kann, wenn andere als beschäftigungsbezogene Zwecke verfolgt werden.

Geht es wie in unserem Beispiel um den Verkauf eines Betriebs oder Unternehmens, so steht nicht die Durchführung des Arbeitsvertrags oder einer anderen Form von Beschäftigung im Vordergrund. Vielmehr werden andere Zwecke erfolgt, so dass Art. 6 Abs. 1 Buchstabe f DSGVO Anwendung finden kann. Soweit das Problem in der Literatur angesprochen wird, geht man im allgemeinen davon aus, dass den Interessen des Kaufinteressenten ausreichend Rechnung getragen ist, wenn er pseudonymisierte oder anonymisierte Daten erhält. Nur bei Führungskräften und Erfindern soll grundsätzlich eine Ausnahme gelten.<sup>16</sup>

In einem weiteren, sehr viel problematischeren Fall wird ebenfalls ein Rückgriff auf Art. 6 Abs. 1 Buchstabe f DSGVO befürwortet.<sup>17</sup> Dabei geht es um die Schaffung eines Algorithmus, der bei Auswahlprozessen für Einstellungen oder Beförderungen zur Anwendung kommen soll. Zuvor werden die erfolgreichsten Führungskräfte und Vertriebsmitarbeiter in ihrem Verhalten analysiert; die Ergebnisse gehen in den Algorithmus

---

<sup>16</sup> Däubler, Gläserne Belegschaften, 2017, Rn. 489d m.w.N.

<sup>17</sup> Hierzu und zum Folgenden Dzida, NZA 2017, 541 ff.

ein. Die Bewerber werden in gleicher Weise „durchleuchtet“. Wer dem firmeneigenen Mitarbeiterideal am nächsten kommt, wird eingestellt bzw. befördert; andere haben keine reale Chance. Auch hier stellt sich die Frage, ob Art. 6 Abs. 1 Buchstabe f im Verhältnis zu den „Best-Arbeitern“ effektiv zur Anwendung kommen kann. Die Detailanalyse ihres (als sehr positiv eingeschätzten) Arbeitsverhaltens macht den Unterschied zu dem eben erörterten Fall der Betriebsveräußerung aus – das spricht dagegen, hier auf Art. 6 Abs. 1 Buchstabe f zurückzugreifen. Der Bezug auf das Arbeitsverhältnis ist sehr viel enger. Ob der Zweck des Beschäftigungsverhältnisses selbst, also § 26 Abs. 1 Satz 1 BDSG-neu auch eine Datenverarbeitung umfasst, die Maßstäbe für andere generieren soll, ist alles andere als evident. Schließlich läuft die vorgeschlagene Prozedur auf die Erarbeitung von Persönlichkeitsprofilen hinaus, was sich nicht mit dem Persönlichkeitsschutz nach dem Grundgesetz vereinbaren lässt.<sup>18</sup>

### **Datenverarbeitung durch die betriebliche Interessenvertretung**

§ 26 Abs. 1 Satz 1 BDSG-neu enthält – in einem Schachtelsatz versteckt – noch eine weitere Ermächtigung. Erlaubt sind danach Datenverarbeitungen, die zur „Ausübung oder Erfüllung“ von Rechten bzw. Pflichten der betrieblichen Interessenvertretungen erforderlich sind. Diese Rechte und Pflichten können sich – was an sich keiner Erwähnung bedurft hätte – aus einem Gesetz, aber auch aus Kollektivvereinbarungen (Tarifverträge, Betriebs- und Dienstvereinbarungen) ergeben. Der Auskunftsanspruch des Betriebsrats nach § 80 Abs. 2 BetrVG und andere Unterrichtsansprüche erhalten so eine datenschutzrechtliche Untermauerung. Die Maßstäbe für die Erforderlichkeit können allerdings unterschiedlich sein, da insoweit dem Betriebsrat ein eigenständiger Beurteilungsspielraum zukommt.<sup>19</sup> § 26 Abs. 1 Satz 1 BDSG-neu hat freilich nicht den Sinn, die Rechte des Betriebsrats einzuschränken, zumal Art. 6 Abs. 1 Buchstabe c DSGVO jede Form von rechtlicher Verpflichtung als Grundlage für eine Verarbeitung anerkennt: Damit sind auch Verpflichtungen gemeint, die sich aus dem BetrVG oder aus Kollektivverträgen ergeben.

### **Zusammenfassung**

Jede Datenverarbeitung bedarf einer Rechtsgrundlage. Diese kann in einer Einwilligung der betroffenen Person liegen, doch spielt diese Möglichkeit in der betrieblichen Praxis nur eine

---

<sup>18</sup> Näher Däubler, Digitalisierung und Arbeitsrecht, 6. Aufl. 2018, § 9 Rn. 24 ff. (im Erscheinen)

<sup>19</sup> Vgl. DKKW-Buschmann, 15. Aufl., § 80 Rn. 83; Fitting, BetrVG, 28. Aufl., § 80 Rn. 51 ff.

relativ geringe Rolle. Wichtigste Basis ist der Vertrag, auf dessen Grundlage gearbeitet wird. Daneben können berechnigte Interessen des Verantwortlichen oder eines Dritten eine Rolle spielen, doch müssen sie sich auf Zwecke beziehen, die nichts mit der vertraglich vereinbarten Arbeit zu tun haben. Die arbeitsrechtliche Sonderregelung des § 26 Abs. 1 BDSG-neu bewegt sich in diesem Rahmen.