Europa regelt den gesamten Datenschutz
- ein Grund zur Freude?

Die Vertreter von EU-Kommission, Ministerrat und Europäischem Parlament haben sich am 15. Dezember 2015 über eine „Datenschutz-Grundverordnung“ geeinigt. Diese enthält nicht nur „Grundsätze“ oder „Richtlinien“, sondern einen bis ins letzte Detail ausformulierten Gesetzestext, der durch umfangreiche Begründungserwägungen ergänzt wird. Er liegt im Augenblick (7.2.2016) nur in englischer Fassung vor; sie ist nicht autorisiert und nicht veröffentlicht. Daneben gibt es eine private deutsche Übersetzung der meisten Artikel. Beides erhält man nur auf dem „kleinen Dienstweg“. Derzeit wird der Text in alle 24 Amtssprachen der EU übersetzt, was bei einem Umfang von gut 300 Seiten einige Zeit in Anspruch nimmt.

Sobald diese Arbeit abgeschlossen ist, fassen Rat und Parlament formelle Beschlüsse, in denen sie das Vereinbarte bestätigen. Anschließend wird die Verordnung im Amtsblatt der EU veröffentlicht; 20 Tage später tritt sie in Kraft. Wirksam wird sie allerdings erst zwei Jahre nach diesem Zeitpunkt – voraussichtlich also im Laufe des ersten Halbjahrs 2018. Sie stellt das Datenschutzrecht auf eine völlig neue Grundlage. Unser vertrautes Bundesdatenschutzgesetz wird in fast allen seinen Teilen der Vergangenheit angehören. Wir sollten deshalb schon heute wissen, was auf uns zukommt, um uns rechtzeitig auf die neue Situation einstellen zu können.

Was bedeutet der Erlass einer EU-Verordnung?

Die Gesetzgebung der EU vollzieht sich in zwei Formen. Die eine ist die Richtlinie, die den Mitgliedstaaten nur bestimmte Ziele vorgibt. Diese müssen dann ein eigenes Gesetz erlassen, um das Gewollte zu realisieren. Dabei verbleibt ihnen meist ein erheblicher Spielraum. Bisher hat die EU im Datenschutz wie im Arbeitsrecht fast nur von diesem Mittel Gebrauch gemacht. Wichtigstes Beispiel ist die geltende Datenschutzrichtlinie vom 24. Oktober 1995[1], doch ist daneben an die Betriebsübergangsrichtlinie oder an die Richtlinien zum Schutz vor Diskriminierungen zu denken.

[1] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, abgedruckt auch bei Däubler/Klebe/Wedde/Weichert, BDSG. Kommentar, 5. Aufl. 2016, Anhang 3

Die Verordnung hat einen anderen Charakter. Sie gilt unmittelbar in jedem Mitgliedstaat und wirkt dort für und gegen jedermann, also auch im Arbeitsverhältnis. Der nationale Gesetzgeber ist im Prinzip ausgeschaltet; nur wo eine Verordnung Lücken lässt oder ihm eine entsprechende Ermächtigung gewährt, kann er noch aktiv werden. Sie ist insoweit einem Bundesgesetz im Verhältnis zu einem Landesgesetz vergleichbar. Und nicht nur das: Die Verordnung geht im Konfliktsfalle dem gesamten nationalen Recht vor. Dies gilt sogar für das Verfassungsrecht, das hinter dem Unionsrecht zurückstehen muss. Die Berufung auf das informationelle Selbstbestimmungsrecht ist beispielsweise nur noch dort möglich, wo das nationale Recht eine Lücke füllen darf. Stattdessen ist in Zukunft das „Recht auf Datenschutz" nach Art 8 der EU-Grundrechtecharta einschlägig, dessen Inhalt noch niemand so recht kennt. Das kann man sehr kritisch sehen (und der Verfasser gehört durchaus zu den Kritikern). Hier soll aber nicht die politische Diskussion fortgeführt, sondern zunächst einmal herausgearbeitet werden, was diese Rechtsänderung konkret für uns bewirkt.

Der Umgang mit einer EU-Verordnung

Da die Verordnung in Deutschland (genauso wie in Spanien oder in Estland) unmittelbar für und gegen jedermann gilt, muss sie bei betrieblichen Auseinandersetzungen, aber natürlich auch von den (Arbeits-)Gerichten beachtet werden. Bei Auslegungsproblemen ist deren Position zunächst maßgebend. Sie können – wenn sie dies für sinnvoll halten - den EuGH einschalten, um von dort eine verbindliche Auskunft zu bekommen. Hat ein Gericht letzter Instanz Zweifel, wie eine Vorschrift genau auszulegen ist, muss es sogar den Rechtsstreit dem EuGH vorlegen. Nur in völlig klaren Fällen darf es darauf verzichten. Im Ergebnis können sich so viele Gerichtsverfahren um rund zwei Jahre verlängern.

Unionsrecht sorgfältig auszulegen, ist eine höchst anspruchsvolle Aufgabe. Es gilt nämlich nicht etwa in Deutschland auf Deutsch, in Frankreich auf Französisch und in Spanien auf Spanisch. Vielmehr sind alle 24 Sprachfassungen gleichermaßen verbindlich. Was geschieht, wenn die Übersetzer nicht aufgepasst haben oder eine Sprache eine bestimmte Nuance nicht zum Ausdruck bringen kann? Dann hat man unterschiedliche Inhalte und die Rechtsanwender müssen sehen, wie sie einen (Auslegungs-)Kompromiss zustande bringen, mit dem alle einigermaßen leben können.[2] In der Praxis gibt es so gut wie niemanden, der alle

[2] Zu dem Beispiel des Begriffs der „Weltanschauung", die in den anderen Sprachfassungen sehr viel mehr Fälle von persönlicher Überzeugung erfasst, s. Däubler NJW 2006,2608 ff.

Unionssprachen beherrschen würde; Genies sind nun mal selten auf dieser Welt. Dies hat zur Folge, dass der EuGH dem Wortlaut bei der Auslegung eine eher geringere Bedeutung beimisst, weil man insoweit oft keine wirklich verlässliche Grundlage hat. Auch die Entstehungsgeschichte ist nicht selten unergiebig. Bei der Datenschutz-Grundverordnung hatten beispielsweise Kommission, Parlament und Rat drei ziemlich weit auseinander gehende Fassungen erstellt, die nunmehr in den Verhandlungen zwischen diesen drei Organen („Trilog" genannt) zusammengeführt wurden. Welches Argument war dafür maßgebend, dass man sich auf eine bestimmte Formulierung einigte? Wahrscheinlich werden wir das nie erfahren – es sei denn im Wege einer Indiskretion („der Vertreter der Kommission war müde und wollte ins Bett, deshalb war er mit dem Vorschlag des Parlamentsvertreters einverstanden"), worauf man sich aber in der Öffentlichkeit nicht berufen kann. Was bleibt sind die Begründungserwägungen, die sich allerdings nicht selten mit einer bloßen Umschreibung des Gesetzestextes oder mit einem Hinweis auf Offenkundiges begnügen. Was bleibt, ist das Abstellen auf den Zweck der Vorschrift. Dabei legen nicht wenige Leute zunächst das in eine Vorschrift hinein, was sie anschließend als „wissenschaftlichen Fund" wieder herausholen und der Fachöffentlichkeit präsentieren.

Die einzelnen Vorschriften sind oft umständlich formuliert und juristisch nicht ganz durchdacht. Dieses „Bürokratensprech" wird uns auf Schritt und Tritt begegnen. Statt zu sagen „Die Einwilligung muss freiwillig und ohne Zwang erfolgen" heißt es etwa in Art. 7 Abs. 4:

„Bei der Beurteilung, ob eine Einwilligung freiwillig erteilt wird, muss dem Umstand größte Beachtung geschenkt werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Bereitstellung eines Dienstes, von der Einwilligung in die Verarbeitung von Daten, die nicht für die Erfüllung dieses Vertrags notwendig sind, abhängig gemacht wird."[3]

Alles klar? Erst nach dreimaliger Lektüre konnte ich die Frage bejahen. Und was bedeutet es juristisch, wenn man einer Angelegenheit „größte" Beachtung schenkt? Würde es schlicht „Beachtung" heißen, wäre dann etwas anderes gemeint?

Nun sind auch deutsche Gesetze nicht immer von bester Qualität. Was wirklich gilt, wird deshalb fast immer durch die Rechtsprechung bestimmt. Ob und unter welchen Umständen Krankheit ein „in der Person liegender Grund" für eine ordentliche Kündigung ist, lässt sich nicht dem Gesetzestext, wohl aber den Entscheidungen des BAG entnehmen. Auch die Frage, wann eine Betriebsräteschulung „erforderlich" im Sinne des § 37 Abs. 6 BetrVG ist, bestimmt

[3] Art. 7 Abs. 4 der Einigung im Trilog (inoffizielle deutsche Übersetzung, die den englischen Originaltext korrekt wiedergibt)

sich nach dem, was in Erfurt entschieden wird. Diese Rolle wird künftig im Datenschutzrecht der EuGH einnehmen. Dieser besteht aus 28 Richtern; jeder Mitgliedstaat entsendet ohne Rücksicht auf seine Bevölkerungszahl eine Person. Diese 28 Menschen kommen aus unterschiedlichen Rechtskulturen. In manchen Ländern sind Urteile sehr kurz, weil der Richter einfach nur sagt: „So ist es!“ Anders bei uns: Hier argumentieren die Gerichte, weil sie auch die Seite überzeugen wollen, die den Rechtsstreit verliert. Das hat den Vorzug, dass die Argumentation oft deutlich macht, wie voraussichtlich in ähnlichen Fällen entschieden wird. Der einzelne Bürger, Arbeitgeber wie Arbeitnehmer gewinnen so Orientierungssicherheit. Der EuGH neigt eher dem ersten Modell zu: Die entscheidenden Ausführungen sind sehr knapp gehalten, oft so knapp, dass man kaum irgendwelche Rückschlüsse ziehen kann. Von „geistiger Schmalkost“ hat deshalb ein deutscher Rechtswissenschaftler gesprochen, was ihm manche Leute sehr übel genommen haben. Wie mir mal ein Mitglied des Gerichts erzählte, sind sich die Richter oft im Ergebnis, nicht aber in der Begründung einig. Was tut man in einem solchen Fall, wenn man viele Fälle zu entscheiden und wenig Zeit für lange Diskussionen hat? Man streicht die kontroversen Passagen einfach aus dem Urteil raus und ist auf diese Weise den Streit los. Den Schaden tragen die betroffenen Bürger: Sie müssen weiter mit Rechtsunsicherheit leben, weil sie nicht vorhersehen können, wie der nächste Fall entschieden wird.

Ergebnis: Das Leben wird nicht einfacher, wenn an die Stelle des BDSG die Datenschutz-Grundverordnung tritt.

Die Inhalte: Verbot mit Erlaubnisvorbehalt und Zweckbindung

Die Verordnung übernimmt viele Inhalte, die aus der Datenschutzrichtlinie und dem BDSG bekannt sind. Sie benutzt allerdings einen weiteren Begriff der „Datenverarbeitung“, zu der nunmehr auch die Erhebung und die Nutzung von Daten gehören.[4] Nach Art. 6 der Einigung ist die Verarbeitung personenbezogener Daten nur dann erlaubt, wenn bestimmte Voraussetzungen erfüllt sind: Einwilligung des Betroffenen, Durchführung eines Vertrages, Wahrung eines berechtigten Interesses, soweit nicht die Interessen, Grundrechte und Grundfreiheiten des Betroffenen überwiegen usw. Eine ähnliche Regelung findet sich heute in § 28 Abs. 1 BDSG. Es bleibt also bei einem „Verbot mit Erlaubnisvorbehalt“. Weiter dürfen Daten nicht gewissermaßen auf Vorrat, für noch unbekannte künftige Verwendungen

[4] Art. 4 Nr. 3 der Einigung

gespeichert werden. Vielmehr verlangt Art. 5 Abs. 1 Buchstabe b der Einigung, dass die Daten „für genau festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden." Ihre Weiterverarbeitung ist grundsätzlich an diesen Zweck gebunden. Eine Ausnahme gilt nur für Zwecke der Statistik, der wissenschaftlichen und historischen Forschung sowie der Archivierung. Diese strikte Zweckbindung wird durch Absatz 3a desselben Artikels wieder stark relativiert; eine Verschlechterung gegenüber dem heute geltenden § 28 Abs. 2 BDSG ist aber nicht ersichtlich.

Die Einwilligung

Welche Voraussetzungen eine wirksame Einwilligung erfüllen muss, lässt sich nur durch Lektüre verschiedener Vorschriften ermitteln. Sie ist einmal definiert in Art. 4 Nr. 8 der Einigung, wo es heißt, Einwilligung des Betroffenen sei eine „jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte eindeutige Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist." Es muss sich also um eine freiwillige Erklärung („ohne Zwang")[5] handeln, bei der der Erklärende über die Umstände voll informiert ist und bei der er seinen Willen „eindeutig" kund tut. Art. 7 der Einigung steht unter der Überschrift „Bedingungen für die Einwilligung", obwohl diese eigentlich schon in der Definition angesprochen sind. Nach Abs. 1 muss die verantwortliche Stelle, nunmehr der „für die Verarbeitung Verantwortliche", nachweisen, dass die Einwilligung vorliegt. Wird sie im Zusammenhang mit einer schriftlichen Erklärung erteilt, so muss das Ersuchen um Einwilligung sich von anderen Erklärungen in dem fraglichen Dokument deutlich unterscheiden und in klarer und einfacher Sprache abgefasst sein. Abs. 3 sieht die Widerruflichkeit jeder Einwilligung mit Wirkung für die Zukunft vor, wobei unklar bleibt, ob dies auch dann gilt, wenn die Einwilligung Teil einer vertraglichen Verpflichtung ist. Abs. 4 ist oben bereits genannt werden – der Inhalt des Art. 7 deckt ersichtlich nicht das ab, was die Überschrift ankündigt.

Individualrechte

[5] Im Englischen heißt es: „freely given"

Der Betroffene muss nach Art. 14a der Einigung eingehend informiert werden, wenn die auf ihn bezogenen Daten bei einem Dritten erhoben werden. Dabei geht die Verordnung über den heutigen § 33 BDSG hinaus und kennt auch weniger Ausnahmen. Auf diese Weise soll mehr Transparenz hergestellt werden. Auch das Auskunftsrecht wird gegenüber § 34 BDSG erweitert, da u. a. auch die Dauer der Speicherung bzw. die Kriterien angegeben werden müssen, nach denen sich die Dauer der Speicherung richtet. Weiter müssen alle verfügbaren Informationen über die Herkunft der Daten mitgeteilt werden. Auf Geheimhaltungsinteressen, die einer Auskunft entgegenstehen könnten, wird in Art. 15 der Einigung nicht hingewiesen. Das erstaunt, da dies etwa im Verhältnis zu Behörden durchaus von Bedeutung sein könnte. Art. 16 gibt ein Recht auf Berichtigung, das anders als in § 35 Abs. 2 Nr. 2 BDSG nur eingreift, wenn die Unrichtigkeit feststeht. Ist sie umstritten, so könnte nach Art. 17a das „Recht auf Einschränkung der Verarbeitung" eingreifen, das der bisherigen Sperrung entspricht, doch ist dies von der Formulierung her nicht ganz eindeutig. Art. 17 enthält das Recht auf Löschung, das unter der Bezeichnung „Recht auf Vergessenwerden" ein hohes Maß an öffentlicher Aufmerksamkeit erlangt hat. Seine wichtigste Folge ist schon heute der Rechtsprechung des EuGH zu entnehmen:[6] Ist eine Information für den Betroffenen negativ, aber in der Gegenwart für die Öffentlichkeit ohne Interesse, so darf eine Suchmaschine nicht mehr auf sie hinweisen. Dies ist sicherlich beifallswert, doch ist keineswegs garantiert, dass der Mantel des Vergessens tatsächlich über die fraglichen Vorgänge gelegt wird: Die Eintragung in einem Register von Personen, deren Gebäude unter Zwangsverwaltung gestellt wurden, blieb in dem entschiedenen Fall unangetastet. Weiter hatte jeder Internetnutzer in der Vergangenheit die Möglichkeit, sich eine Kopie von der Eintragung anzufertigen. Von einem wirksamen Datenschutz im Internet sind wir noch weit entfernt[7] - daran wird auch die Verordnung nichts ändern.

Betrieblicher Datenschutzbeauftragter

Die Pflicht, einen betrieblichen Datenschutzbeauftragten zu bestellen, besteht nach der Verordnung sehr viel seltener als nach dem BDSG. Es gibt sie nach Art. 35 Abs. 1 nur bei Behörden und öffentlichen Einrichtungen sowie dann, wenn die Verarbeitung sensitiver Daten (z. B. über die Gesundheit) oder das regelmäßige und systematische Beobachten und Beurteilen von Personen („Monitoring") zur „Kerntätigkeit" des Unternehmens gehört. Letzteres meint vermutlich Auskunfteien. Wo der „Kern" endet, bleibt unklar und wird

[6] EuGH 13. 5. 2014 – C-131/12 – NJW 2014, 2257 – Google Spain
[7] Näher Däubler AiB EXTRA Sonderausgabe März 2015 S. 29 ff.

sicherlich den EuGH beschäftigen. Abs. 4 gibt den Mitgliedstaaten allerdings das Recht, auch für andere Unternehmen betriebliche Datenschutzbeauftragte vorzuschreiben, so dass die Regelung des BDSG erhalten bleiben kann. Der Datenschutzbeauftragte darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden (Art. 36 Abs. 3). Ob dies auch den heute bestehenden Kündigungsschutz erfasst? Wohl eher nicht. Man könnte allenfalls versuchen, den Schutz vor Benachteiligungen durch den nationalen Gesetzgeber in diesem Sinne zu konkretisieren. Auch hier liegt das letzte Wort beim EuGH. Die Aufgaben des Datenschutzbeauftragten sind ähnlich wie im BDSG bestimmt.

Datenübermittlung in Drittstaaten

Seit der Safe-Harbor-Entscheidung des EuGH[8] ist die Datenübermittlung in Drittstaaten zu einem Problem geworden, das nicht nur die Spezialisten, sondern die breite Öffentlichkeit interessiert. Der vorliegende Text enthält allerdings keine unmittelbaren Hinweise, wie der aktuelle Konflikt mit den USA zu lösen ist. Die Art. 40 bis 44 der Einigung folgen im Prinzip dem bisher geltenden Recht,[9] enthalten allerdings eine Reihe neuer Akzente. Wie bisher wird zwischen Drittländern mit angemessenem und solchen mit nicht angemessenem Datenschutz unterschieden. Die Tatsache, dass der EuGH in der Safe-Harbor-Entscheidung die „Angemessenheit" wie „Gleichwertigkeit" gelesen hat, findet im Text keinen Niederschlag. Neu ist, dass die Angemessenheit auch für bestimmte Teile eines Landes (z. B. eine kanadische Provinz) oder einen bestimmten Wirtschaftssektor festgestellt werden kann. Dies leuchtet durchaus ein, wenn man bedenkt, dass möglicherweise das Bankgeheimnis in den USA sehr gut gewahrt ist, während in anderen Bereichen keinerlei Abschirmung personenbezogener Daten existiert. Ob der Datenschutz in einem Drittland angemessen ist oder nicht, muss regelmäßig, mindestens alle vier Jahre, überprüft werden – auch dies ist eine bisher nicht vorhandene Regelung.

Ist der Datenschutz in einem Drittland nicht als „angemessen" anerkannt, kann die Datenübermittlung grundsätzlich nur auf der Grundlage „geeigneter Garantien" erfolgen. Diese können wie bisher grundsätzlich aus Standardvertragsklauseln oder aus verbindlichen unternehmensinternen Regeln („binding corporate rules") bestehen, wobei die Anforderungen an letztere in Art. 43 detailliert umschrieben sind. Bemerkenswert ist Art. 43a der Einigung, wonach Entscheidungen von Gerichten oder Verwaltungsbehörden eines Drittstaats, die eine

[8] 6. 10. 2015 – C-362/14 – NZA 2015, 1373
[9] Dazu Däubler/Klebe/Wedde/Weichert-Däubler Erläuterungen zu §§ 4b und 4c

Übermittlung bestimmter Daten anordnen, nur dann vollstreckt werden dürfte, wenn ein Rechtshilfeabkommen besteht. Ähnlich wie heute nach § 4c Abs. 1 BDSG können daneben in Sonderfällen wie Einwilligung des Betroffenen oder Erfüllung eines mit dem Betroffenen geschlossenen Vertrages Daten in ein unsicheres Drittland übermittelt werden.

Aufsichtsbehörde

Die Stellung der Aufsichtsbehörde hat in den Artikeln 46 bis 54 eine eingehende Regelung erfahren. Ihre Anordnungsbefugnisse sind in Art. 53 Abs. 1b der Einigung sehr viel detaillierter aufgeführt als in § 38 Abs. 5 BDSG und überdies gegenüber dem bisherigen Recht erweitert worden. Sie ist sogar befugt, bestimmte Datenverarbeitungsvorgänge zu verbieten und eine Geldbuße zu verhängen, die bei bestimmten Verstößen bis zu 10 Mio. Euro oder bis zu 2 % des weltweiten Jahresumsatzes eines Unternehmens gehen können. Auch die grenzüberschreitende Zusammenarbeit ist eingehend geregelt.

Arbeitnehmerdatenschutz

Einer der umstrittensten Punkte war während der gesamten Vorarbeiten die Vorschrift des Art. 82 und die darin enthaltene „Öffnungsklausel“ zugunsten des Arbeitnehmerdatenschutzes. Die Endfassung gestattet den Mitgliedstaaten, „spezifischere Regelungen“ in Bezug auf Arbeitnehmerdaten „im Beschäftigungskontext“ zu schaffen, und zwar durch Gesetz oder durch Kollektivvereinbarungen, was nach Erwägungsgrund 124 auch „works agreements“, also Betriebsvereinbarungen umfasst. Dabei ist die Einstellung wie die Beendigung des Arbeitsverhältnisses sowie seine Durchführung erfasst, die (in eher überflüssiger Weise) mit zahlreichen Worten umschrieben wird. Die „spezifischen Regeln“ müssen geeignete Maßnahmen enthalten, um die Menschenwürde, die Grundrechte und sonstige legitime Interessen der Arbeitnehmer zu schützen, wobei auf die Transparenz der Datenverarbeitung, die Datenübermittlung im Konzern sowie auf Überwachungssysteme am Arbeitsplatz besonders zu achten ist.

Was sind „spezifischere“ Regeln oder „more specific rules“? Hier wird es besonders naheliegen, auch die anderen Sprachfassungen heranzuziehen, die möglicherweise mehr Aufschluss geben können. Ist beispielsweise eine Regelung, die den Einsatz von GPS-Systemen zur Überwachung von Außendienstmitarbeitern verbietet, eine „spezifischere“

Datenschutzbestimmung? Um wie steht es mit dem Massen-Screening von E-Mails? Kann im Arbeitsverhältnis von den allgemeinen Voraussetzungen der Einwilligung abgewichen und diese beispielsweise nur dann zugelassen werden, wenn es um einen Vorgang geht, der ganz oder überwiegend dem Arbeitnehmer nützt? Wie steht es mit arbeitnehmerähnlichen Personen und weiteren Gruppen von Beschäftigten, die durch § 3 Abs. 11 BDSG in den Arbeitnehmerdatenschutz des § 32 BDSG einbezogen wurden? Muss man sie in Zukunft wieder ausklammern, weil der englische Begriff „employee“ keine solche Erweiterung kennt? Die Frage soll hier nur aufgeworfen und kann erst bei Vorliegen des endgültigen Textes beantwortet werden.

Fazit

Das EU-Recht lässt sich sehr viel schwerer als nationales Recht handhaben; es werden sich zusätzliche Rechtsunsicherheiten ergeben. Inhaltlich garantiert die Verordnung ein ordentliches Datenschutzniveau. Eine Verbesserung auf nationaler Ebene sieht sich insofern einem zusätzlichen Hindernis ausgesetzt, als der freie Verkehr personenbezogener Daten in der Union nach Art. 1 Abs. 3 der Einigung nicht über die Verordnung hinaus eingeschränkt werden darf. Damit ist ein statisches Element in einem Bereich eingebaut worden, in dem sich fast täglich neue Probleme ergeben. Die Änderung der Verordnung ist in einem Staatenverbund von 28 Mitgliedern ein problematisches Unterfangen.

Nicht ausreichend erfasst ist weiter der Datenschutz im Internet, wie er etwa unter dem Stichwort des „eingebauten Verfallsdatums“ diskutiert wird. Auch die Verordnung geht noch von einer Art „Rechenzentrumsmodell“ aus: Es gibt eine verantwortliche Stelle, die irgendwo in der Union eine Niederlassung besitzt, und die bestimmte Verhaltensregeln zu beachten hat. Doch was geschieht, wenn sich auf einem kleinen Inselstaat in der Karibik ein Server und eine Bedienungsmannschaft befinden, die gegen Zahlung eines bestimmten Betrages Auskunft über viele EU-Bürger geben? Durch fleißiges „Abgreifen“ von Daten könnten zahlreiche Profile verfügbar sein.

Was schließlich fehlt, ist ein Hinweis darauf, dass sich die Arbeit immer mehr auf das Internet verlagert: Eine totale Erfassung des Arbeitnehmerverhaltens wird dann zum Regeltatbestand und ist nicht mehr nur Entscheidung eines „überwachungssüchtigen“ Arbeitgebers. Das

Verbot von Persönlichkeitsprofilen wird in der digitalen Gesellschaft zur zwingenden Notwendigkeit.

Prof. Dr. Wolfgang Däubler, Bremen