ZDH
ZENTRALVERBAND DES DEUTSCHEN HANDWERKS

Stellungnahme

zur

Europäischen Datenschutz-Grundverordnung

Abteilung Recht
Berlin, April 2012

DAS HANDWERK
DIE WIRTSCHAFTSMACHT. VON NEBENAN.

Allgemeine Aspekte

Einheitlichkeit des europäischen Datenschutzrechts

Der Entwurf für eine europäische Datenschutz-Grundverordnung zielt maßgeblich darauf ab, einen europaweit einheitlichen Standard zum Schutz personenbezogener Daten einzuführen. Anders als in anderen Rechtsgebieten erscheint die Gewährleistung eines einheitlichen Schutzniveaus innerhalb der Europäischen Union beim Datenschutz sinnvoll und geboten.

Datenströme machen im Rahmen moderner Datenverarbeitung nicht an nationalen Grenzen Halt. Innerhalb eines Bruchteils von Sekunden können immense Datensätze global versendet, verarbeitet und genutzt werden. Angesichts dieses Ausmaßes, können die zum Teil stark voneinander abweichenden und nicht aufeinander abgestimmten Regelungen der Mitgliedstaaten keinen adäquaten Regelungsrahmen bieten.

Dies gilt für den Schutz des Betroffenen ebenso wie für die zulässige Datennutzung durch die Wirtschaft. Betriebe, die äußerst hohe nationale Datenschutzanforderungen zu erfüllen haben, erfahren einen nicht unerheblichen Wettbewerbsnachteil gegenüber Betrieben aus Mitgliedstaaten, die keine über das Datenschutzniveau der EU hinausreichenden Vorschriften kennen. Datenschutz stellt insofern einen nicht unerheblichen Wettbewerbsfaktor dar.

Die angestrebte verstärkte Europäisierung des Datenschutzrechts geht deshalb auch unter dem Gesichtspunkt eines gleichberechtigten Wettbewerbs im europäischen Binnenmarkt grundsätzlich in die richtige Richtung.

Nicht überzeugend stellt sich indes die unterschiedslose Behandlung von privaten und öffentlichen Stellen dar. Die Absicht zur Vereinheitlichung der gegenwärtig inkohärenten Rechtslagen in den Mitgliedstaaten umfasst sowohl den privatwirtschaftlichen als auch den öffentlich-rechtlichen Bereich. Während sich eine verstärkte Angleichung des Datenschutzes im privatwirtschaftlichen Bereich für Betroffene und Betriebe aus den genannten Gründen durchaus als vorteilhaft erweisen würde, erschließt sich die Notwendigkeit einer Vereinheitlichung im behördlichen Bereich nicht. Öffentliche Stellen sind unmittelbar an die europäischen Grundrechte gebunden und damit zur Wahrung des Grundrechts auf Schutz der personenbezogenen Daten (Artikel 8 Charta der Grundrechte der Europäischen Union) verpflichtet.

Es ist nicht ersichtlich, dass in dieser Hinsicht ein uneinheitlicher Schutzstandard oder gar Defizite in einzelnen Mitgliedstaaten bestehen. Insofern bedarf es zumindest diesbezüglich keiner gezielten und erst recht keiner – wie noch zu zeigen sein wird – absoluten Vereinheitlichung des Datenschutzes.

Die Ausrichtung des Verordnungsentwurfs auf eine vollständige Harmonisierung des Datenschutzrechts sollte sich vor diesem Hintergrund auf den privatwirtschaftlichen Sektor beschränken. Dem steht eine Angleichung der datenschutzrechtlichen Bestimmungen für den behördlichen Bereich nicht entgegen. Jedoch sollte den Mitgliedstaaten im öffentlich-rechtlichen Bereich weiterhin die Möglichkeit zur national-individuellen Normierung überlassen bleiben.

Verhältnismäßigkeit der Verordnung

Die Kommission zieht zum Zweck der Vereinheitlichung des Datenschutzrechts das Regelungsinstrument der Verordnung heran. Dies ist mit Blick auf die unmittelbare Wirkung und den für gewöhnlich abschließenden Regelungscharakter einer Verordnung konsequent. So besteht kein Zweifel daran, dass mithilfe einer Verordnung die europaweite Einheitlichkeit des Datenschutz-

rechts gewährleistet wird und die Verordnung somit ein geeignetes Regelungsinstrument ist. Allerdings ist fraglich, ob eine Verordnung als Instrument zur Erreichung des angestrebten Zwecks auch tatsächlich erforderlich und damit verhältnismäßig ist.

Nach Artikel 5 Abs. 4 S. 1 EUV darf die Union die ihr eingeräumte Kompetenzen nur dann ausüben, wenn sie eine Handlungsform wählt, die nicht nur geeignet ist, das Regelungsziel zu erreichen, sondern zudem den Mitgliedstaaten einen größtmöglichen Handlungsspielraum überlässt. Gerade diese Voraussetzung der Verhältnismäßigkeit kann beim vorliegenden Entwurf nicht ohne Weiteres bejaht werden.

Die Verordnung führt zu einem absolut vereinheitlichten Schutzniveau. Nationale Regelungen dürfen nur dann aufrecht erhalten oder künftig erlassen werden, wenn sie äußerst strenge Voraussetzungen erfüllen (vgl. Artikel 6 Absatz 3). Im Ergebnis müssen nationale Ermächtigungsgrundlagen zur Datennutzung dem von der Verordnung exakt vorgegebenen Datenschutzniveau entsprechen. Abweichungen sind weder nach unten noch nach oben zulässig. Dementsprechend ist selbst die einzelstaatliche Normierung eines höheren Schutzniveaus untersagt.

Der normative Handlungsspielraum der Mitgliedstaaten wird hierdurch nahezu vollständig ausgehöhlt. Die Verordnung begründet insoweit in ihrer vorgesehenen Gestaltung die strikteste und einschränkenste Form der hier zur Auswahl stehenden Regelungsmöglichkeiten. Die Erforderlichkeit einer derart strikten Regelungsintensität ist im Ergebnis zu bezweifeln. Die angestrebte Einheitlichkeit des Datenschutzniveaus in Europa bedarf keiner allumfassenden und in allen Detailfragen unmittelbar geltenden Bestimmungen. Das Regelungsinstrument einer Richtlinie kommt hier als milderes, aber ebenso effizientes Mittel in Betracht. Dies gilt insbesondere mit Blick auf den öffentlichen Bereich, der – wie oben dargelegt – keiner vollständigen Harmonisierung bedarf. Zumindest für diesen Bereich erscheint die Heranziehung einer Verordnung in der vorgesehenen inhaltlichen Gestaltung unverhältnismäßig im Sinne von Artikel 5 Abs. 4 EUV.

Konzept der personenbezogenen Daten als Regelungsproblem

Das Begriffspaar „personenbezogene Daten“ steht im Zentrum der Datenschutzkonzeption der Verordnung. Damit hält der Entwurf an der konzeptionellen Ausrichtung der Richtlinie von 1995 fest und entspricht Artikel 8 der Charta der Grundrechte der Europäischen Union.

Inwieweit die Aufrechterhaltung dieses Anknüpfungspunkts allerdings geeignet ist, den absehbaren Anforderungen des Datenschutzrechts zu genügen, ist durchaus fraglich. Nach der Definition des Artikel 4 Absatz 2 des Entwurfs handelt es sich bei personenbezogenen Daten um alle Informationen, die sich auf eine Person beziehen. Dieser sehr weit gefassten Begriffsbestimmung liegt der Gedanke zugrunde, dass es kein unerhebliches personenbezogenes Datum gibt, da jede Information in Verbindung mit anderen Daten eine verwertbare Aussage bis hin zur Erstellung eines persönlichen Profils ermöglicht.

Der nach diesem Verständnis gesetzlich zu garantierende Schutz jeder Information, die sich auf eine Person bezieht, ist bereits heute faktisch nicht mehr umsetzbar. Die Ursachen hierfür sind vielschichtig. Ein maßgeblicher Grund ist jedoch die Erweiterung des öffentlichen Raums durch neue Medien und das Internet. Ein zunehmend unbeschwerter Umgang der Betroffenen mit ihren Daten in der Öffentlichkeit ist bereits seit langem zu beobachten. Folgerichtig ist es zur Selbstverständlichkeit geworden, gewisse Informationen über Personen im Internet einholen zu können.

Die herkömmliche Datenschutzkonzeption, die undifferenziert die Nutzung jeder Art von personenbezogenen Daten unter Erlaubnisvorbehalt stellt, kann mit der rasanten Entwicklung nicht mit halten. Die Folge ist eine stetig erforderliche nachträgliche Anpassung der gesetzlichen Erlaubnistatbestände an die veränderten Realitäten.

Der vorliegende Entwurf ist unterm Strich ebenfalls nur ein weiterer Versuch, die gesetzlichen Grundlagen an die Entwicklung seit 1995 anzupassen. So ist die Verordnung nach Aussage der Kommission im Wesentlichen darauf gerichtet, der technischen Entwicklung und hierbei insbesondere dem rasanten Erfolg sozialer Netzwerke und moderner Medien datenschutzrechtlich Herr zu werden.

Die Haltwertszeit der Verordnung wird voraussichtlich den Gesetzgebungsprozess überdauern. Es ist jedoch absehbar, dass die Regelungen alsbald einer erneuten Anpassung an die weitere technische, aber auch an die gesellschaftliche, Entwicklung bedürfen werden. Vor diesem Hintergrund liegt der Gedanke nahe, dass die Kommission mit dem Festhalten an ihrer herkömmlichen Datenschutzkonzeption eine Chance zur wirklichen Modernisierung des Datenschutzes vertan hat.

Es erscheint dringend geboten, die Wirksamkeit und Effizienz des gegenwärtigen Datenschutzkonzepts auf den Prüfstand zu stellen. Gerade soziale Netzwerke werden das künftige Kommunikationsverhalten und Datenbewusstsein der Betroffenen verstärkt prägen. Es spricht gegenwärtig viel dafür, den Datenschutz auf einen Schutzkern der Privat- und Intimsphäre zu konzentrieren, anstatt weiterhin sämtliche Daten gleichwertig gesetzlich schützen zu wollen.

Aus Sicht des Handwerks wäre es ein wichtiger Schritt, die insgesamt groß angelegte Reform ebenfalls für eine Diskussion über zukunftsfähige Datenschutzkonzepte zu nutzen. Rat und Europäisches Parlament sind nun aufgefordert, als Gesetzgeber die Weichen für ein wirklich modernes und tragfähiges Datenschutzrecht zu stellen.

Rechtssicherheit vor Flexibilität – Einschränkung der delegierten Rechtsakte

Aus dem herkömmlichen Datenschutzkonzept folgt ein stetiger Anpassungsbedarf der gesetzlichen Vorschriften an die sich verändernden Realitäten. Um diesem kontinuierlichen Nachbesserungsbedarf entgegenzuwirken, versucht die Kommission sich mehr Handlungsflexibilität zu verschaffen. Durch eingeräumte Ermächtigungen zum Erlass von delegierten Rechtsakten soll es der Kommission möglicht werden, schnell und flexibel auf sich abzeichnende Entwicklungen zu reagieren.

Das Wesen von delegierten Rechtsakten ist dem Grunde nach gut geeignet, der Kommission ein flexibles Regelungsinstrument an die Hand zu geben, ohne hierfür jeweils ein langwieriges Gesetzgebungsverfahren durchlaufen zu müssen. Aufgrund des mangelnden Rechtsetzungsverfahrens sollte dieser Weg der Normsetzung allerdings nur im Einzelfall und sehr gezielt eingesetzt werden. Eine allzu umfassende und nahezu Rechtsbereichs ausschöpfende Anwendung delegierter Rechtsakte erscheint dagegen allein aus Gesichtspunkten demokratischer Legitimität nicht unbedenklich.

Aber gerade dies ist das Ansinnen der Kommission bei der vorliegenden Reform. Der Entwurf sieht bei gerade einmal 91 Artikeln insgesamt 26 Ermächtigungsgrundlagen für den Erlass delegierter Rechtsakte vor. Dabei ist nahezu jeder Regelungsbereich der Verordnung betroffen. Die Kommission lässt sich mit den zahlreichen Ermächtigungsklauseln das Recht einräumen, die

in der Verordnung normierten Bestimmungen näher zu regeln.

Das quantitative und inhaltliche Ausmaß der vorgesehenen Befugnisse der Kommission zum Erlass von delegierten Rechtsakten ist nicht nur aus Gründen guter Gesetzgebung abzulehnen. Die von der Kommission angestrebte Regulierungsflexibilität führt kehrseitig zu einer nicht unerheblichen Rechtsunsicherheit. Die am Ende des Rechtsetzungsprozesses in Kraft tretenden Vorschriften stellen im Ergebnis nur noch einen Regelungsrahmen dar, der im Nachfolgenden durch delegierte Rechtsakte der Kommission ausgestaltet werden wird.

Gleichgültig, ob es sich um die Voraussetzungen zur rechtmäßigen Datennutzung, die Bereitstellung bereichsspezifischer Informationen oder den Umfang von Dokumentationspflichten handelt: Welche spezifischen Regelungen die Kommission im Nachgang erlassen wird, ist nicht absehbar. Betrieben ist es vor diesem Hintergrund nicht möglich, sich mittelfristig auf gesetzliche Datenschutzanforderungen einzustellen und diese in betriebwirtschaftlich adäquate Weise in die betrieblichen Prozesse einzupflegen. Stetige Umstellungen der datenschutzrelevanten Maßnahmen bei internen Betriebsabläufen, AGB oder im Rahmen von Auftragsdatenverarbeitungen führen dagegen zu einem immensen Aufwand, der vor allem für kleine und Kleinstbetriebe finanziell und personell kaum zu bewältigen ist.

Das deutsche Handwerk steht für einen modernen und effizienten Datenschutz. Maßgeblich hierfür sind insbesondere Klarheit und Verlässlichkeit der datenschutzrechtlichen Vorschriften. Die angestrebte Reform des europäischen Datenschutzrechts darf nicht auf der Ungewissheit künftig zu erlassender delegierter Rechtsakte beruhen. Dies gilt insbesondere dann, wenn das vermeintliche Erfordernis von flexibleren Regelungsinstrumenten das Resultat einer nicht zukunftsfähigen Datenschutzkonzeption ist.

Betriebe wie Betroffene müssen wissen, welche Rechte und Pflichten die gesetzlichen Vorschriften künftig vorsehen. Der gegenwärtige Entwurf wird dieser Anforderung nicht gerecht und ist aufgrund der damit einhergehenden Rechtsunsicherheit insbesondere für Kleinstbetriebe nicht handhabbar und damit für das Handwerk in diesem Punkt nicht hinnehmbar.

Regelungsaspekte im Einzelnen

Grundsätze schärfen

Die in Kapitel 2 geregelten Grundsätze und Ermächtigungsgrundlagen für eine zulässige Verarbeitung personenbezogener Daten sind durch eine nachvollziehbare Regelungssystematik geprägt. Rechtsanwendern wird hierdurch grundsätzlich ein praxisgerechter Umgang mit den Vorschriften ermöglicht.

Unklar ist jedoch der an erster Stelle normierte Grundsatz von Treu und Glauben. Dieses offensichtlich dem Artikel 8 der Charta der Grundrechte der Europäischen Union entlehnte Prinzip ist weder seiner Zielrichtung noch seiner materiellrechtlichen Wirkung nach verständlich. Die Übertragung des Grundsatzes in das Sekundärrecht führt zudem deshalb zu Schwierigkeiten, weil der Grundsatz von Treu und Glauben auch in anderen Rechtsbereichen Bedeutung erlangt. In dem gegenwärtig diskutierten Entwurf für ein Gemeinsames Europäisches Kaufrecht (GEK) soll der Grundsatz von Treu und Glauben nicht nur das Vertragsverhältnis der Parteien in grundlegender Weise prägen, sondern bei entsprechender Missachtung zu konkreten Rechtsfolgen führen. Anders als im hier vorliegenden Verordnungsentwurf, wird der Begriff „Treu und Glauben“ beim GEK definiert. Eine entsprechende Begriffsbestimmung wäre auch im Rahmen der Datenschutzverordnung geeignet, Klarheit zu erzeugen. Allerdings wäre ein von der Definition

des GEK abweichendes Begriffsverständnis im Sinne der Einheitlichkeit der Rechtsordnung nicht wünschenswert.

Erläuterungsbedürftig ist ebenfalls der Grundsatz des Artikel 5 Buchst. E), wonach Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglichen soll. Gespeicherte Daten, die eine Identifizierung des Betroffenen nicht ermöglichen, sind irreversibel anonymisiert. Derart anonymisierte Daten lassen keine Rückschlüsse auf den ursprünglich Betroffenen zu und sind daher datenschutzrechtlich unbedenklich. Weshalb also die stets mögliche Identifizierung ein Prinzip des Datenschutzes sein soll, bleibt unklar.

Erlaubnistatbestände praxisgerecht gestalten

Die Normierung der jeweiligen Ermächtigungstatbestände sind – mit Ausnahme einzelner Aspekte – klar formuliert und dürften für den durchschnittlichen Rechtsanwender im Ergebnis verständlich sein.

Die für die Betriebspraxis wichtigste Regelung, wonach Daten zum Zweck der Vertragserfüllung oder zur Durchführung vorvertraglicher Maßnahmen genutzt werden dürfen (Artikel 6 Abs. 1 Buchstab. b), wird jedoch maßgeblich eingeschränkt. So dürfen Daten zur Durchführung vorvertraglicher Maßnahmen nur dann genutzt werden, wenn die Maßnahmen „auf Antrag der betroffenen Person erfolgen“. Unklar ist, was im Sinne dieser Norm unter einem „Antrag“ zu verstehen ist. Sowohl dessen Form, als auch sein inhaltlicher Gegenstand ergeben sich nicht aus dem Verordnungsentwurf.

Hinzu kommt, dass die Erfüllung gesetzlich vorgeschriebener vorvertraglicher Pflichten nicht von etwaigen Anträgen oder Zustimmungen abhängig gemacht werden kann. Im Rahmen von Verbraucherverträgen hat der Unternehmer dem Verbraucher z. B. im Vorfeld des Vertragsschlusses eine Reihe von Informationen auszuhändigen. Erfolgt die Information via E-Mail, muss der Unternehmer die E-Mail Adresse des Verbrauchers und damit ein personenbezogenes Datum nutzen, um seiner gesetzlichen Pflicht nachzukommen. Inwiefern und worauf gerichtet der Verbraucher in diesem Zusammenhang einen Antrag stellen muss, ist nicht nachzuvollziehen.

Sollten die vorvertraglichen Informationspflichten jedoch künftig von einem – wie auch immer gearteten Antrag – des Verbrauchers abhängen, führt dies allein zu einer weiteren Verkomplizierung der ohnehin schon vertheoretisierten und nicht mehr praxisgerechten Formalanforderungen von Vertragsschlüssen mit Verbrauchern.

Im Übrigen zielen die sehr eng gefassten Erlaubnistatbestände darauf ab, die Einwilligung des Betroffenen als faktische Regelgrundlage für Datenverarbeitungen zu etablieren. Die Möglichkeit zur Einholung einer Einwilligung des Betroffenen soll nach Maßgabe des Entwurfs jedoch dann ausgeschlossen sein, wenn zwischen der Position der verantwortlichen Stelle und der des Betroffenen ein erhebliches Ungleichgewicht besteht (Artikel 7 Abs. 4). Wann ein solches Ungleichgewicht gegeben sein soll und ob sich die Fälle, wie nach bisheriger Methodik auf Ober-Unter-Ordnungsverhältnisse – z. B. arbeitsrechtliche Beziehungen – beschränkt, bleibt unklar.

Zudem ist fraglich, ob der offensichtlich hinter dieser Norm stehende Schutzgedanke dem Betroffenen tatsächlich nutzt. Durch die Vorschrift wird die Handlungsfreiheit des Betroffenen faktisch in nicht unerheblicher Weise eingeschränkt. Denn selbst dann, wenn der Betroffene mit der Verarbeitung seiner Daten einverstanden ist oder dies sogar wünscht, ist es der „übermächtigen“ verantwortlichen Stelle nicht möglich, die Daten zu nutzen. Anstelle eines gesetzlichen Schutzes, der die Handlungsfreiheit des Betroffenen einschränkt, sollte dem Betroffenen mehr Eigenver-

antwortlichkeit eingeräumt werden. Der ZDH warnt vor einer allzu starken gesetzlichen Bevormundung des Betroffenen, deren negativen Auswirkungen sich im Verbraucherrecht bereits niedergeschlagen haben.

Eine allzu enge Fokussierung auf die Einwilligung als Ermächtigungstatbestand wird dem Interesse des Betroffenen insgesamt nicht gerecht. Nach den beabsichtigten Regeln muss künftig jeder für alles und jeden kleinsten Einzelfall eine gesonderte Einwilligung erklären. Dass dies auch oder gerade in besonderer Weise aus Sicht des Betroffenen zu einem lästigen Formalismus, aber keineswegs zu mehr Bewusstsein und Kontrolle über den Umlauf seiner personenbezogenen Daten führt, ist absehbar. Davon abgesehen stehen viele Kundendienstleistungen, die eine Datennutzung erfordern, im eindeutigen Interesse des Betroffenen. Kfz-Werkstätten, die ihren Bestandskunden beispielsweise einen Erinnerungshinweis bezüglich des nächsten TÜV-Termins zukommen lassen, müssen hierfür zwangsläufig die Daten des Kunden verwenden. Da dieser Service jedoch offensichtlich im Interesse des Kunden steht, ist es nicht nachvollziehbar, weshalb der Kunden auch für diesen Fall gesondert einwilligen muss. Deshalb wäre es praxis- und interessensgerecht, die Erhebung und Nutzung von Daten dann zu gestatten, wenn die Datenverwendung offenkundig im Interesse des Betroffenen steht. Sollte dies trotz anzunehmenden Interesses nicht der Fall sein, stände dem Betroffenen der Widerspruch zu. Der Artikel 6 sollte um einen solchen praktisch relevanten Erlaubnistatbestand ergänzt werden.

Verarbeitung besonderer Daten möglich machen

Der Entwurf unterscheidet besondere Kategorien von personenbezogenen Daten von gewöhnlichen Daten und stellt deren Verarbeitung unter strengere Voraussetzung. Die Unterscheidung ist aufgrund der Sensibilität und Intimität der Daten grundsätzlich gerechtfertigt. Allerdings müssen auch bei besonderen Daten die Interessen von Betroffenen und Betrieben gewahrt bleiben und einer verhältnismäßigen Regelung unterstellt werden.

In diesem Zusammenhang schießen die Voraussetzungen zur Verarbeitung von Gesundheitsdaten weit über das Ziel hinaus. Nach Maßgabe des Artikel 81 Abs. 1 Buchst. a) dürfen Gesundheitsdaten nur durch Personen verarbeitet werden, die entweder der ärztlichen oder einer sonstigen gesetzlichen Geheimhaltungspflicht unterstehen. Demzufolge müssten Augenoptiker oder Hörgeräteakustiker mangels gesetzlich angeordneter Geheimhaltungspflicht ärztliches Fachpersonal zur Verarbeitung der Gesundheitsdaten ihrer Kunden einstellen oder für jeden Einzelfall eine Einwilligung einholen. Dass dies in keiner Weise praktikabel oder verhältnismäßig ist, liegt auf der Hand. Es bedarf dementsprechend einer praxisgerechten Lösung, die z. B. darin bestehen kann, dass sämtliche Mitarbeiter des Betriebs eine Verschwiegenheitserklärung zu unterzeichnen haben, um Gesundheitsdaten der Kunden verarbeiten zu dürfen.

Weitere Kategorien besonderer Daten schaffen

Ebenso wie eine Differenzierung von besonders sensiblen Daten erscheint es mit Blick auf die eingangs beschriebene gesellschaftliche Entwicklung im Umgang mit gewissen – in der Regel allgemein zugänglichen – Daten angemessen, Kategorien von Daten herauszustellen, deren Verarbeitung unter erleichterten Voraussetzungen möglich ist. Dies ist typischerweise bei Kontakt- und Adressdaten der Fall. Die Erfahrungen mit dem deutschen Datenschutzrecht haben gezeigt, dass etwaige Erleichterungen bei der Nut-

zung von Listendaten den Anforderungen der Praxis gerecht zu werden, ohne dabei den Schutz der Betroffenen zu verringern.

Gerade vor dem Hintergrund, dass der Verordnungsentwurf weiterhin an dem herkömmlichen Konzept der personenbezogenen Daten festhält, empfiehlt es sich, Erleichterungen für bestimmte – in der Regel öffentliche – Datenkategorien einzuführen, um der Praxis notwendige Handlungsmöglichkeiten an die Hand zu geben, ohne den Betroffenenschutz anheim zu stellen.

Rechte der Betroffenen

Das erreichte Ausmaß von Datenverarbeitungen und Informationsströmen führt zu einer zunehmenden Komplexität, die der jeweils Betroffene im Einzelfall nicht mehr überblicken kann. Es ist deshalb richtig, dass der Entwurf in Kapitel 3 den Transparenzgedanken im Datenschutzrecht normativ aufgreift. Die im Einzelnen vorgesehenen Maßnahmen zielen jedoch darauf ab, Betriebe mit einem unverhältnismäßigen Bürokratismus und Betroffene mit Informationen zu konfrontieren, die sie weder benötigen noch wünschen.

Maßgeblich für die absehbar negativen Folgen für Betriebe und Betroffene ist der konzeptionelle Ansatz, dass Betriebe jedem Betroffenen unaufgefordert zahlreiche Informationen zur Datenverarbeitung mitteilen müssen. Es erscheint regelrecht absurd, Transparenz und Klarheit durch eine Informationsflut schaffen zu wollen. Anstelle den Betroffen – unabhängig, ob dieser die Informationen wünscht oder nicht – über zum Teil kleinteilige Detailinformationen zu unterrichten (insb. Artikel 14), sollte dem Betroffenen lediglich die Auskunft darüber erteilt werden, dass ihm diese Informationen zuteil werden, wenn er es wünscht.

Die Kommission läuft Gefahr, mit diesem Ansatz dieselben konzeptionelle Fehlentwicklung wie im Verbraucherrecht in Gang zu setzen. Die immer ausführlicheren Informationspflichten, die den Verbraucher im Ergebnis mehr verunsichern als helfen und ihm insbesondere keine Orientierung bieten, zeigen eindrucksvoll, dass ein pures Streben nach informationeller Quantität keinem der Beteiligten nutzt.

Das deutsche Handwerk spricht sich mit Nachdruck dafür aus, die im Entwurf vorgesehenen Informationspflichten, nicht nur mit Blick auf ihren jeweiligen informativen Mehrwert auf den Prüfstand zu stellen, sondern vor allem die Mitteilungspflicht von einem zuvor gestellten Antrag des Betroffenen abhängig zu machen. Anderenfalls werden insbesondere Verbraucher künftig durch Informationen aus Verbraucher- und Datenschutzrecht regelrecht belästigt.

Datenschutz durch formalisierten Bürokratismus?

Neben den zahlreichen Informationspflichten obliegen den verantwortlichen Stellen laut Entwurf weitere Handlungspflichten, mit deren Hilfe der Schutz des Betroffenen sichergestellt werden soll. Wenngleich das Ziel dieser Pflichten unstreitig wichtig ist, sollten im Sinne eines gerechten Interessensausgleichs nicht nur das Ziel, sondern ebenfalls die Effektivität und Verhältnismäßigkeit der zur Zielerreichung einzusetzenden Mittel in Betracht gezogen werden. Die im Entwurf vorgesehenen umfassenden Dokumentations-, Prüf- und Genehmigungspflichten lassen jedoch insgesamt eine Ausgewogenheit der Zweck-Mittel-Relation vermissen.

Dass selbst die Kommission von einer enormen, mit den Pflichten einhergehenden bürokratischen Belastung ausgeht, verdeutlicht die Ausnahmevorschrift für KMU. Es ist positiv hervorzuheben,

dass die Kommission mit Blick auf die Leistungsfähigkeit kleiner und mittlerer Betriebe in diesem Zusammenhang dem „*Think Small First*"-Prinzip Ausdruck verleiht. Dasselbe gilt hinsichtlich der Anforderungen zur notwendigen Bestellung von betrieblichen Datenschutzbeauftragten.

Die gezielte und in diesem konkreten Fall richtige Ausnahme von KMU kann jedoch nichts an dem grundsätzlich unverhältnismäßigen Pflichtenkatalog für verantwortliche Stellen ändern. Dies gilt umso mehr, als die Ausnahmeregelung für KMU lediglich die Dokumentationspflicht des Artikel 28 betrifft. Die vom Entwurf verlangte Datenschutz-Folgenabschätzung sowie insbesondere das behördliche Genehmigungsverfahren nach Artikel 34 findet ungeachtet der personellen und finanziellen Möglichkeiten in gleicher Weise Anwendung auf Kleinstbetriebe wie auf global agierende Konzerne oder staatliche Einrichtungen. Es ist nicht ersichtlich, weshalb es für jede Form der Datenverarbeitung unabhängig der Kategorie von Daten einer vorherigen Genehmigung durch die Aufsichtsbehörden bedürfen sollte. Soweit sich der Zweck dieser für Betriebe und Behörden als kaum zu bewältigender Bürokratismus darstellende Genehmigungspflicht darin erstreckt, dass – wie Absatz 2 der Norm formuliert – die Einhaltung der Verordnung sichergestellt werden soll, steht dies offensichtlich außer Verhältnis zum Aufwand.

Ein derartiges Missverhältnis zwischen Aufwand und Zweck kann unter keinem Gesichtspunkt rechtfertigt werden. Der ZDH fordert diesbezüglich eine deutlich spürbare Entbürokratisierung der Dokumentations-, Prüf- und Genehmigungspflichten.

Keine kollektive Rechtsdurchsetzung

Artikel 76 des Verordnungsentwurfs sieht vor, dass auch Verbraucherverbände die Rechte einzelner oder mehrer Betroffener geltend machen können sollen. Der darin verankerte Ansatz für einen kollektiven Rechtsschutz im Datenschutzrecht ist entschieden abzulehnen. Zum einen obliegt es ausschließlich den Betroffenen selbst, für die Durchsetzung ihrer Rechte einzutreten und die ihnen zur Verfügung stehenden Rechtswege auszuschöpfen. Die stellvertretende Beauftragung professioneller Klägerverbände durch Gesetz wird dem Prinzip der Eigenverantwortung nicht gerecht und markiert eine falsche Weichenstellung hinsichtlich der weiteren Entwicklung des europäischen Prozessrechts.

Zum anderen werden Bemühungen zur Einführung kollektiver Rechtsschutzmechanismen der gesamtgesellschaftlichen Verantwortung des Gesetzgebers nicht gerecht, so lange den unstreitig mit Sammelklagen verbundenen Problemen nicht adäquat begegnet und vorgesorgt werden kann. Dies ist jedoch nach wie vor unvermindert der Fall. Weder die Gefahr von Erpressungspotenzialen noch das Problem von unweigerlich auftretenden wirtschaftlichen Interessen von Klageverbänden zur Anstrengung von selbst unbegründeten Klagen sind nicht einmal annähernd ausgeräumt. Der ZDH warnt vor den unabsehbaren Folgen eines immer weiter angelegten kollektiven Rechtsschutzes und spricht sich mit Nachdruck für eine Streichung des in Artikel 76 normierten ausgeweiteten Verbandsklagerechts aus.

Architektur der Aufsichtsbehörden

Der Verordnungsentwurf greift nicht nur sämtliche datenschutzrelevante Aspekte der Datenverarbeitung auf, sondern zudem in die Organisationsstruktur der Aufsichtsbehörden ein. Die in Kapitel 6 angeordneten Anforderungen an die organisatorischen Strukturen sowie an die personelle und rechtliche Gestaltung der Aufsichts-

behörden lassen im Ergebnis nur sehr wenig Spielraum für einzelstaatliche Regelungen.

Ob und inwieweit diese Regelungstiefe der Aufsichtsbehörden durch die Verordnung erforderlich ist, darf bezweifelt werden. Insbesondere erscheint die vorgeschriebene Bestimmung, wonach im Fall mehrerer bestehender Aufsichtsbehörden eine dieser Behörden zur Überwachung der anderen zu bestimmen ist, mit Blick auf föderal organisierte Mitgliedstaaten nicht unproblematisch.

Ebenfalls kritisch zu betrachten ist der vom Entwurf vorgesehene Aufgabenkatalog der Aufsichtsbehörden. Nach Artikel 52 sollen Aufsichtsbehörden über die originäre Überwachungsfunktion zusätzlich rechtsberatend gegenüber Betrieben und sonstigen verantwortlichen Stellen tätig werden. Es ist absehbar, dass diese Aufsichtsbehörden mit einem derart weit gefassten Aufgabenspektrum – zumindest in ihrer gegenwärtigen Gestaltung – personell und funktional überfordert wären. Hinzu kommt, dass es einer solch intendierten Aufgabenerweiterung zu einer Monopolisierung der datenschutzrechtlichen Beratung führt, da Rechtsberatung und anschließende staatliche Kontrolle in einer Hand vereint wären. Dies ist bereits aus ordnungspolitischen Gründen verfehlt und abzulehnen.

Anders verhält es sich mit der beabsichtigten Einführung eines Europäischen Datenschutzausschusses. Dieses Gremium ist grundsätzlich geeignet, die kohärente Einhaltung und Anwendung des künftigen europäischen Datenschutzes zu fördern.

Fazit

Mit dem vorliegenden Entwurf versucht die Kommission, das europäische Datenschutzrecht umfassend und dem Grunde nach auch abschließend zu regeln. Die dabei angestrebte Vereinheitlichung des Datenschutzrechts ist mit Blick auf zum Teil erhebliche und nicht zu rechtfertigende Unterschiede in den Mitgliedstaaten zumindest für den privatwirtschaftlichen Bereich zu begrüßen. Die zugleich angestrebte Vereinheitlichung des öffentlichen Bereichs, die zugleich die Organisationsgestaltung der Aufsichtsbehörden umfasst, erscheint in dem vorgesehenen Maß weder erforderlich noch verhältnismäßig und ist deshalb im Ergebnis abzulehnen.

Inhaltlich ist der Entwurf durch zahlreiche Ermächtigungsgrundlagen zum Erlass von delegierten Rechtsakten geprägt, die sehr viele Fragen zur künftigen Gestaltung des europäischen Datenschutzrechts offen lassen und für Betroffene und Verantwortliche zu einer nicht unerheblichen Rechtsunsicherheit führen. Hier muss deutlich nachgebessert und für mehr Rechtssicherheit und Rechtsklarheit gesorgt werden.

Stark überarbeitungsbedürftig sind ebenfalls die ineffizienten und größtenteils außerordentlich bürokratischen Pflichten für die verantwortlichen Stellen. Die Kommission scheint den Betroffenenschutz mit exakt denselben Mitteln wie den Verbraucherschutz vorantreiben zu wollen. Dass dies in eine Sackgasse von immer mehr Informationspflichten und formalisierter Bürokratie endet, die unterm Strich nicht einmal dem Betroffenen hilft, zeigt die Entwicklung des Verbraucherrechts. Dieser Entwicklung muss von Beginn an ein Riegel vorgeschoben werden. Anstelle quantitativer Informations-, Prüf- und Genehmigungspflichten müssen effektive und gezielte Schutzmechanismen das künftige Datenschutzrecht prägen.

Der ZDH plädiert für eine umfassende Angleichung des Datenschutzes im privaten Bereich, warnt jedoch vor den Folgen einer eindimensionalen und bürokratisch konzipierten Datenschutzpolitik. Der vorliegende Entwurf bietet die Chance, ein modernes, den absehbaren techni-

schen und gesellschaftlichen Entwicklungen Rechnung tragendes Datenschutzrecht in ganz Europa einzuführen. Damit dieses vom deutschen Handwerk unterstützte Vorhaben tatsächlich gelingt, bedarf es an den genannten Stellen gezielter, aber auch zum Teil umfassender Änderungen. Rat und Europäisches Parlament sind aufgerufen, ihrer diesbezüglichen Verantwortung gerecht zu werden und die Weichen für ein zukunftsfähiges, gesamteuropäisches Datenschutzrecht zu stellen.