

Stellungnahme

Stellungnahme des HDE zum Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU)

Stand: 21.03.2017



I. Einleitung

Der Handelsverband Deutschland (HDE) ist die Spitzenorganisation des deutschen Einzelhandels für rund 400.000 selbstständige Unternehmen mit insgesamt drei Millionen Beschäftigten und jährlich 430 Milliarden Euro Umsatz. Der Einzelhandel ist nach Industrie und Handwerk der drittgrößte Wirtschaftszweig in Deutschland. Der HDE hat 100.000 Mitgliedsunternehmen aller Branchen, Standorte und Größenklassen.

Im Einzelhandel nehmen datenbasierte Geschäftskonzepte eine immer größere Rolle ein – nicht nur im Online-Handel, sondern auch im stationären Handel. Für Einzelhändler und Handelsunternehmen stellen sich mit dem Inkrafttreten der Datenschutzgrundverordnung viele Fragen im Hinblick auf die künftige Zulässigkeit bisheriger datenschutzrelevanter Geschäftsabläufe. Die bestehende Rechtsunsicherheit ist groß. Es ist daher zu begrüßen, dass die Bundesregierung noch in dieser Legislaturperiode eine Anpassung des Bundesdatenschutzgesetzes anstrebt. Es ist unbedingt erforderlich, dass möglichst frühzeitig die rechtlichen Rahmenbedingungen abschließend festgelegt werden, um die Grundlage für die Anpassung der Unternehmensprozesse zu schaffen. Anderenfalls müsste eine weitere Umstellung an ein späteres Gesetz erfolgen, das neue Kosten für die Unternehmen verursachen würde. Aus Sicht des HDE sollte das Ziel verfolgt werden, die Rechtssicherheit und Rechtsklarheit zu erhöhen, ohne die Möglichkeiten der Datenverarbeitung, die die Grundverordnung beinhaltet zu beschränken. Die Übernahme einiger Regelungen aus dem aktuell geltenden Bundesdatenschutzgesetz stellt hierfür in einigen Fällen eine praktikable Regelungsmöglichkeit dar, wenn insoweit eine bewährte Praxis beibehalten werden kann. Nationalgesetzliche Verschärfungen des Datenschutzniveaus lehnen wir ab. Sie widersprechen dem Vollharmonisierungsgedanken der Grundverordnung.

Von besonderer Bedeutung für den Handel sind insbesondere folgende Vorschriften des Gesetzentwurfs, auf die näher eingegangen werden soll:

- § 4: Videoüberwachung
- § 24: Verarbeitung zu anderen Zwecken
- § 26: Datenverarbeitung im Beschäftigungskontext
- § 31: Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften
- § 32: Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
- § 33: Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

II. Zu den Vorschriften im Einzelnen

1. Videoüberwachung, § 4 Abs. 1 BDSG-E

Die Regelung des § 4 BDSG-E entspricht inhaltlich weitgehend der Regelung des bisherigen BDSG nach der aktuell in den Beratungen befindlichen Änderungen durch das Videoüberwachungsverbesserungsgesetz, zu dem der HDE ebenfalls eine Stellungnahme abgegeben hat. Darin haben wir bereits dargelegt, dass die restriktive Auslegung der Datenschutzaufsichtsbehörden in der Praxis des Einzelhandels zu großen Problemen und hohen Bürokratiekosten für Einzelhändler und Handelsunternehmen führt.



a) Löschungsfrist

Im Einzelhandel ist die Videoüberwachung zum Zweck des Eigentumsschutzes als berechtigtes Interesse nach § 6 b Absatz 1 Nummer 3 BDSG der mit Abstand häufigste Anwendungsfall. Dabei verlangen die Datenschutzaufsichtsbehörden eine Löschung in der Regel nach spätestens 48 Stunden. Teilweise werden die Aufnahmen bereits nach 24 Stunden überschrieben. In begründeten Einzelfällen, z. B. wenn wegen Feiertagen kein Geschäftsbetrieb erfolgt, billigen die Aufsichtsbehörden zwar eine geringfügig längere Speicherfrist zu. Dies ist aber in der Praxis nur von geringer Bedeutung, weil das Umprogrammieren der gesamten Videoüberwachungsanlage vor einem an ein Wochenende angrenzenden Feiertag einen zu großen Aufwand verursachen würde. In diesem Zusammenhang ist auch zu erwähnen, dass die Datenschutzaufsichtsbehörden das automatische Löschen der Aufzeichnungen durch ein Selbstüberschreiben als wirksamste Art des Löschens empfehlen. Die Datenschutzaufsichtsbehörden gehen davon aus, dass innerhalb von 48 Stunden geklärt sei, ob die weitere Aufbewahrung des aufgezeichneten Videomaterials wegen erfolgter Überfälle und Diebstähle noch erforderlich ist. Dies mag bei offen begangenen Delikten, wie einem Überfall einer Tankstelle, zwar der Fall sein. Ladendiebstähle werden jedoch gerade in der Regel nicht offen begangen, so dass sie in vielen Fällen gerade nicht sofort bemerkt werden. Wenn diese jedoch mit einer zeitlichen Verzögerung von wenigen Tagen bemerkt werden, ist die Speicherfrist oft bereits abgelaufen und sind die Aufnahmen überschrieben. Im Rahmen von Ermittlungen zu Straftaten, die nicht unmittelbar im Geschäft verübt werden, fordern Ermittlungsbehörden oft Aufzeichnungen aus Ladengeschäften an. Diese können aufgrund der kurzen Löschungsfrist regelmäßig nicht mehr zur Verfügung gestellt werden. Eine Verlängerung der Speicherfrist ist daher unbedingt erforderlich. Die maximale Frist sollte so bemessen sein, dass die praktische Möglichkeit besteht, dass Videoaufzeichnungen den Strafverfolgungsbehörden während der Ermittlungen zur Verfügung gestellt werden können. Dies ist derzeit nicht der Fall. Der Bundesrat hat vorgeschlagen, dass eine Löschung der Aufzeichnungen innerhalb von 7 Tagen stets als unverzüglich gelten soll. Gleichzeitig hat er den Regelungsvorschlag allerdings auf die Videoüberwachung von öffentlich zugänglichen Anlagen und Einrichtungen des öffentlichen Verkehrs, für die eine Sonderregelung mit dem Videoüberwachungsverbesserungsgesetz eingeführt worden ist, beschränkt (BR-Drs. 110/17(B), Ziffer 8). Der Vorschlag ist grundsätzlich zu begrüßen, sollte aber nicht nur auf einige Anwendungsfälle beschränkt sein, sondern für die Videoüberwachung insgesamt gelten.

b) Erweiterung der Rechtsgrundlagen

Es soll aber auch darauf hingewiesen werden, dass die Videoüberwachung im Einzelhandel aktuell auch anderen Restriktionen unterliegt. Zum einen darf die Videoüberwachung überhaupt nur als Ultima Ratio eingesetzt werden. Zudem wird von den Aufsichtsbehörden verlangt, dass die Erforderlichkeit belegt wird, das heißt, dass zunächst Straftaten abgewartet werden müssen, bevor eine Videoüberwachung zulässig ist. Keinesfalls darf eine flächendeckende Überwachung erfolgen, weil die Kunden keiner vollständigen Überwachung ausgesetzt sein dürfen. Die Videoüberwachung ist daher auf bestimmte Bereiche oder Gänge zu begrenzen, in denen besonders oft Diebstähle passieren. Dies führt dazu, dass Diebstähle in andere Bereiche des Geschäfts verlagert werden, teilweise werden die gleichen Produkte nur an einer anderen Stelle eingesteckt.

Allgemeine Sicherheitsbelange sowie der Schutz von Kunden und Mitarbeitern werden bisher zumindest von einigen Aufsichtsbehörden nicht als Grund für eine Videoüberwachung anerkannt. Dies liegt daran, dass der Erlaubnistatbestand des § 6 b Absatz 1 Nummer 3 BDSG (Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke) so ausgelegt wird, dass allein berechnete Interessen des datenschutzrechtlich Verantwortlichen, also des Unternehmens oder des Einzelhändlers selbst, darunter subsumiert werden können. Erfasst sind grundsätzlich zwar der Schutz des Eigentums des Händlers und auch dessen Schutz, wenn er etwa selbst im Laden mitarbeitet. Nicht erfasst ist jedoch der Schutz von Mitarbeitern und Kunden vor Angriffen. Ebenso wenig erfasst ist der Wunsch, allgemein an der Aufklärung von Straftaten mitzuwirken.

Dies steht in einem eklatanten Widerspruch zu den Wünschen der Mitarbeiter, Kunden und Sicherheitsbehörden. Beschäftigte sind bei Überfällen als Erste betroffen und leiden oft lange an den körperlichen und psychi-



schen Folgen des Überfalls. Kunden fordern die Mitwirkung an gegen sie gerichtete Straftaten offensiv ein und geben Unternehmen teilweise eine Mitschuld, wenn z. B. ein Teil eines Geschäfts nicht überwacht war oder die Aufnahmen nicht mehr vorliegen, wenn im Rahmen der Ermittlungen darauf zugegriffen werden soll. Anfragen von Sicherheitsbehörden erfolgten in aller Regel erst nach Ablauf der Speicherfrist, z. T. erst Wochen nach der Straftat. Anfragen werden oft gestellt im Zusammenhang mit Straftaten, die nicht gegen den Einzelhändler gerichtet waren. Wenn Außenbereiche überwacht werden, z. B. weil Leergut draußen gelagert wird, werden Aufnahmen angefordert, weil Ermittlungen ergeben haben, dass ein Täter diesen Bereich vor der Tat oder auf der Flucht passiert hat. Selbst bei schweren Straftaten kann kein Beitrag mehr zur Strafverfolgung geleistet werden, wenn die Speicherfrist abgelaufen ist und die Ermittlungsbehörden sich nicht sofort an den Händler wenden.

Unter diesen Gesichtspunkten ist die Fortführung der bisherigen Rechtslage im Moment zwar aus Gründen der Rechtssicherheit akzeptabel. Sie stellt jedoch lediglich eine Konkretisierung der Regelung des Art. 6 Abs. 1 Buchstabe f) der Verordnung (EU) 2016/679 dar und kann diese nicht einschränken. Der HDE hält angesichts der restriktiven Auslegung des § 6 b BDSG a. F. und der damit für den Einzelhandel verbundenen Probleme größere Spielräume zum Schutz des Eigentums und der körperlichen Unversehrtheit von Mitarbeitern und Kunden für erforderlich. Es wird daher genau zu beobachten sein, ob die Regelung des § 4 Abs. 1 BDSG-neu nicht zu unvereinbaren Einschränkungen gegenüber der Datenschutzgrundverordnung führt und daher angepasst oder aufgehoben werden muss.

Ungeachtet dessen halten wir es angesichts der heute bestehenden Einschränkungen bei der Durchführung von Videoüberwachung im Einzelhandel weiterhin für erforderlich, den Anwendungsbereich für die durch das Videoüberwachungsverbesserungsgesetz eingefügte Regelung des § 4 Abs. 1 Nr. 2 BDSG-E nicht nur auf Einkaufszentren zu begrenzen. Einzelhandelsgeschäfte, z. B. Waren- und Kaufhäuser, große Fachhandelsgeschäfte und Selbstbedienungsmärkte, unterliegen oft der gleichen Sicherheitslage wie Einkaufszentren. Gerade in Innenstadtlagen ist die Frequenz oft sehr hoch. Zudem würden Wertungswidersprüche entstehen, wenn einerseits bei einigen hochfrequentierten öffentlich zugänglichen Einrichtungen zu recht der Schutz von Leben, Gesundheit und Freiheit von sich dort aufhaltenden Personen als wichtiges öffentliches Interesse bei der Interessenabwägung in besonderem Maße zu berücksichtigen sein soll, dies aber im ebenso hochfrequentierten Einzelhandel außerhalb von Einkaufszentren nicht in gleichem Maße gelten würde.

Wir schlagen hierfür folgende Formulierung für § 4 Absatz 1 Satz 2 vor:

„Bei der Videoüberwachung von

1. öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsorten, Einkaufszentren und Einzelhandelsgeschäften oder Parkplätzen, oder

2. Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs,

gilt der Schutz von Leben, Gesundheit oder Freiheit von dort aufhaltenden Personen als ein besonders wichtiges Interesse.“

c) Kennzeichnung der Videoüberwachung

Nach § 4 Absatz 2 BDSG-E sind der Umstand der Beobachtung, der Name und die Kontaktdaten des Verantwortlichen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen. Die Pflicht zur Kenntlichmachung „zum frühestmöglichen Zeitpunkt“ ist nicht nachzuvollziehen. Der Begründung nach soll den Betroffenen dadurch die Möglichkeit gegeben werden, sich frühzeitig auf den Umstand der Videoüberwachung einzustellen. Durch eine vorgelagerte Information würde aber nicht mehr deutlich, in welchem Bereich die Videoüberwachung tatsächlich erfolgt. Die Information für die Betroffenen würde daher sogar verschlechtert.



Dies könnte nämlich so verstanden werden, dass wenn beispielsweise in einem Einkaufszentrum der Eingangsbereich videoüberwacht wird, eine Information über die Videoüberwachung künftig bereits an der Zufahrt zum Parkplatz zu erfolgen hätte, auch wenn der Parkplatz gar nicht überwacht wird. Wir halten es für sehr viel klarer und transparenter, wenn – der bisherigen Regelung entsprechend – die Bereiche gekennzeichnet werden, in denen eine Videoüberwachung auch tatsächlich erfolgt. Die Formulierung, dass die Videoüberwachung „durch geeignete Maßnahmen“ erkennbar zu machen ist, ist vollkommen ausreichend, um eine sachgerechte Information der Betroffenen zu erreichen.

Zudem führt die Pflicht zur Angabe der Kontaktdaten dazu, dass alle Schilder, die auf eine Videoüberwachung hinweisen, ausgetauscht werden müssten. Dies würde einen erheblichen zusätzlichen Aufwand verursachen. Bei der Videoüberwachung im Einzelhandel ist jedoch offensichtlich, durch wen die Überwachung erfolgt. Das Verkaufspersonal ist für alle Kunden unmittelbar ansprechbar, die Adresse für jeden ohne weiteren Aufwand zu ermitteln. Die Pflicht zur Angabe der Kontaktdaten bringt also keinen zusätzlichen Nutzen für Betroffene, verursacht jedoch einen großen bürokratischen Aufwand.

§ 4 Absatz 2 BDSG-E sollte daher keinesfalls über die bisherige Formulierung des § 6 b Abs. 2 BDSG hinausgehen. Wir schlagen folgende Formulierung vor:

„Der Umstand der Beobachtung ist durch geeignete Maßnahmen kenntlich zu machen.“

2. Verarbeitung zu anderen Zwecken durch nicht-öffentliche Stellen, § 24 BDSG-E

Die Möglichkeiten der Nutzung von Daten für einen anderen als den ursprünglichen Erhebungszweck sind im Gesetzentwurf der Bundesregierung gegenüber dem Referentenentwurf stark eingeschränkt worden. Die nach dem BDSG bestehende Zulässigkeit der Zweckänderung aufgrund eines berechtigten Interesses ist nun nicht mehr vorgesehen. Zulässig ist neben den unmittelbar in der Verordnung geregelten Fällen nur noch eine zweckändernde Verarbeitung zur Gefahrenabwehr oder Strafverfolgung sowie zur Rechtsdurchsetzung.

Zwar ist die effektive Geltendmachung und Durchsetzung von Ansprüchen insbesondere beim Kauf auf Rechnung im Fernabsatzgeschäft sehr wichtig, so dass es sich um eine richtige Konkretisierung handelt.

Die zweckändernde Datenverarbeitung sollte nach Auffassung des HDE – wie im Referentenentwurf vorgesehen – jedoch auch möglich sein, wenn dafür ein berechtigtes Interesse des Verantwortlichen und – darüber hinaus – auch eines Dritten besteht.

Welche Zwecke nach der Datenschutzgrundverordnung als vereinbar mit dem ursprünglichen Erhebungszweck bei Kundendaten angesehen werden, ist derzeit noch nicht geklärt. Zur Herstellung von Rechtssicherheit ist es daher erforderlich, die berechtigten Interessen des Verantwortlichen als Grundlage für eine zweckändernde Datenverarbeitung zuzulassen. Beispiele für die Erforderlichkeit der zweckändernden Datenverarbeitung aufgrund eines berechtigten Interesses sind folgende:

- Nicht erst zur Verfolgung, sondern bereits für die Verhinderung und Erkennung von Straftaten ist es erforderlich, bei klar definierten Auffälligkeiten Daten von einzelnen Kunden einer näheren Überprüfung zu unterziehen. Dies kann bspw. erforderlich sein, um etwa im Bereich des Online-Handels bei begründetem Anlass organisierte Kriminalität (z. B. Betrug oder Cyberkriminalität) aufzudecken. Anderenfalls können den Handelsunternehmen erhebliche finanzielle Schäden entstehen. Hierbei handelt es sich um



ein berechtigtes Interesse des Verantwortlichen, vgl. Erwägungsgrund 47 der Verordnung (EU) 679/2016.

- Auch Kostenvorteile der Verantwortlichen oder die Optimierung des eigenen Leistungsangebotes sind grundsätzlich berechnete Interessen gemäß § 23 Abs. 2 Nr. 3 BDSG-E. Etwa können bereits erhobene personenbezogene Daten unter Umständen herangezogen werden, um Geschäftsprozesse zu automatisieren und zu synchronisieren (z. B. im Controlling und Reporting) oder die Kundenansprache und das Serviceangebot zu verbessern (z. B. im Online-Handel).
- Auch für Direktwerbung sollten die Daten mindestens in dem Rahmen genutzt werden dürfen, wie es aktuell im Bundesdatenschutzgesetz vorgesehen ist. Auch dies ist als berechtigtes Interesse in Erwägungsgrund 47 der Datenschutzgrundverordnung anerkannt.

Wir schlagen daher vor, die Regelung des Referentenentwurfs wieder vollumfänglich in das Gesetz aufzunehmen.

Der Bundesrat fordert, die Weiterverarbeitung von Daten zur Geltendmachung, Ausübung oder Verteidigung von rechtlichen Ansprüchen einzuschränken und auf Ansprüche des Verantwortlichen gegenüber der betroffenen Person zu reduzieren (BR-Drs. 110/17 (B), Ziffern 22 und 23). Dieser Vorschlag ist abzulehnen. In Rechtsstreitigkeiten spielen oft auch die Rechtsverhältnisse zu Dritten eine Rolle. Zeugen sind regelmäßig Dritte, deren Daten selbstverständlich weiterhin zum Zweck der Geltendmachung, Ausübung oder Verteidigung von rechtlichen Ansprüchen weiterverarbeitet werden müssen. Die vom Bundesrat behauptete Gefahr für Verbraucherinnen und Verbraucher ist dagegen nicht nachvollziehbar. Die Erforderlichkeit der Weiterverarbeitung zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche unterliegt der Kontrolle der Aufsichtsbehörden und muss demzufolge plausibel dargelegt werden können.

3. Datenverarbeitung für Zwecke des Beschäftigtenverhältnisses, § 26 BDSG-E

Ausweislich der Gesetzesbegründung führt § 26 die spezialgesetzliche Regelung des heutigen § 32 BDSG lediglich fort. Dies trifft im Grundsatz zu, allerdings soll der Beschäftigtendatenschutz im Rahmen der Neuregelung auch noch um zahlreiche Aspekte erweitert werden. Aufgrund des bereits sehr hohen Schutzniveaus im Bereich des Beschäftigtendatenschutzes in Deutschland wird diese Ausweitung vom HDE insgesamt sehr kritisch bewertet.

Zu den wichtigsten Änderungen im Bereich Beschäftigtendatenschutz im Einzelnen:

a) Einwilligung

In § 26 Absatz 2 sollen zusätzliche Anforderungen an die Einwilligung im Beschäftigtenverhältnis geschaffen werden. So sollen besondere Maßstäbe für die Freiwilligkeit festgelegt werden. Im Regelfall soll zudem die Schriftform für eine Einwilligung im Beschäftigtenverhältnis erforderlich sein. Über den Zweck der Datenverarbeitung und das Widerrufsrecht sollen Beschäftigte in Textform aufgeklärt werden müssen.

Die Regelung in § 26 Absatz 2 ist überflüssig und muss daher gestrichen werden. Aufgrund der konkreten Regelungen zur Zulässigkeit von Einwilligungen in der Datenschutz-Grundverordnung (u. a. in Art. 6 u. 7; Erwägungsgrund 32) sind zusätzliche Ausführungen hierzu im nationalen Gesetz nicht erforderlich. Hinzu kommt, dass auch das Bundesarbeitsgericht (BAG, Urt. v. 11.12.2014 – 8 AZR 1010/13) bereits ausdrücklich



bestätigt hat, dass die Erteilung einer Einwilligung im Beschäftigungsverhältnis möglich ist. Wird die Regelung dennoch umgesetzt, wäre insbesondere die Regelung in Satz 2 dringend zu korrigieren, da das Erfordernis der „Freiwilligkeit“ an viel zu enge Voraussetzungen geknüpft wird, die noch dazu zu unbestimmt sind. Das Erfordernis der „Freiwilligkeit“ im Sinne dieser Vorschrift wäre damit in der Praxis kaum zu erfüllen. Hinzu kommt, dass man die Arbeitgeber auch noch mit erheblichen Rechtsunsicherheiten zurücklassen würde. Außerdem geht das Schriftformerfordernis für die Einwilligung in Satz 3 über die Vorgaben aus der Datenschutz-Grundverordnung hinaus, die dafür kein entsprechendes Formerfordernis vorsieht (siehe hierzu insbesondere Erwägungsgrund 32). Das gilt auch für die Regelung in Satz 4, nach der der Arbeitgeber Beschäftigte in Textform über den Zweck der Datenverarbeitung und über das Widerrufsrecht informieren muss.

Sollte entgegen der hier vertretenen Ansicht dennoch an der Regelung festgehalten werden, sollte das Formerfordernis für die Einwilligung zumindest auf die Textform nach § 126 b BGB reduziert werden. Angesichts des Rechts des Beschäftigten, die Einwilligung jederzeit zu widerrufen, sind besondere Schutzvorkehrungen, die ein Schriftformerfordernis rechtfertigen würden, nicht erforderlich. Für die Nachweisbarkeit und die Dokumentation der Einwilligung reicht die Textform aus. Gerade für Unternehmen mit vielen Standorten würde das Schriftformerfordernis einen erheblichen bürokratischen Zusatzaufwand bedeuten, ohne dass dem ein entsprechender Nutzen gegenüberstünde.

b) Kollektivvereinbarungen

Die Regelung in § 26 Absatz 4 stellt nunmehr klar, dass Kollektivvereinbarungen weiterhin Rechtsgrundlage für Regelungen zum Beschäftigtendatenschutz bilden können. Von dem Begriff „Kollektivvereinbarungen“ sind ausweislich der Gesetzesbegründung zu § 26 Absatz 4 die in der Praxis wichtigen Regelungsinstrumente Tarifverträge und Betriebs- und Dienstvereinbarungen umfasst.

Die nunmehr in § 26 Absatz 1 aufgenommene zusätzliche Ergänzung „oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarungen) ergebenden Rechte und Pflichten der Interessenvertretungen der Beschäftigten“ ist überflüssig und sollte daher in jedem Fall gestrichen werden. Einzig die in diesem Passus ebenfalls enthaltene Legaldefinition des Begriffs der Kollektivvereinbarungen ist richtig und wichtig. Diese muss daher direkt in § 26 Absatz 4 aufgenommen werden.

c) Beschäftigtenbegriff

Nach § 26 Absatz 8 Nr. 1 sollen auch Zeitarbeitnehmer im Verhältnis zum Entleiher Beschäftigte im Sinne des Gesetzes sein. Diese Ausweitung des Beschäftigungsbegriffs ist überflüssig und abzulehnen. Zum einen haben Zeitarbeitnehmer in Deutschland bereits ein vollwertiges Arbeitsverhältnis mit allen Rechten und Pflichten gegenüber ihrem Arbeitgeber, dem Verleiher. Zum anderen steht dem Zeitarbeitnehmer bereits nach heutiger Rechtslage im Verhältnis zum Entleiher das Recht auf informationelle Selbstbestimmung zu, so dass er auch in diesem Verhältnis über die Verwendung personenbezogener Daten bestimmen kann.

d) Verdeckte Videoüberwachung

In der Gesetzesbegründung zu § 26 heißt es nunmehr wörtlich: „Der Gesetzgeber behält sich vor, Fragen des Datenschutzes im Beschäftigungsverhältnis innerhalb dieser Vorschrift oder im Rahmen eines gesonderten Gesetzes konkretisierend bestimmte Grundsätze, die im Rahmen der Rechtsprechung zum geltenden Recht bereits angelegt sind, zu regeln. Dies gilt insbesondere für den (...) expliziten Ausschluss von heimlichen Kon-



trollen im Beschäftigungsverhältnis (...)“. Nach ständiger BAG-Rechtsprechung (z. B. BAG, Urt. vom 21.06.2012 – 2 AZR 153/11; BAG, Urt. vom 22.09.2016 – 2 AZR 848/15) kann die verdeckte Videoüberwachung im Einzelfall zulässig sein. Dies ist zur Aufdeckung von Straftaten im Einzelhandel (z. B. Kassenmanipulationen) von extrem hoher Bedeutung. Das Bundesarbeitsgericht hat die Voraussetzung dafür in jahrelanger Rechtsprechung hinreichend konkret bestimmt, so dass für die Einzelhandelsunternehmen derzeit ein hohes Maß an Rechtssicherheit beim Einsatz von verdeckter Videoüberwachung besteht. Ein gesetzliches Verbot stünde daher in einem krassen Widerspruch zur ständigen Rechtsprechung des Bundesarbeitsgerichts. Auch die gesetzliche Kodifizierung der vom Bundesarbeitsgericht aufgestellten Zulässigkeitsvoraussetzungen für eine verdeckte Videoüberwachung wäre abzulehnen. Eine solche Neuregelung wäre vor dem Hintergrund der bestehenden Rechtsprechung nicht nur überflüssig, sondern auch kontraproduktiv, da dies lediglich zu neuer Rechtsunsicherheit führen würde.

4. Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten (§ 29 BDSG-E)

Nach § 29 BDSG-E werden Informations-, Auskunfts- und Benachrichtigungsrechte des Betroffenen eingeschränkt, wenn das Geheimhaltungsinteresse eines Dritten an den sonst zu offenbarenden Informationen überwiegt. Auch die Befugnisse der Aufsichtsbehörden werden gemäß § 29 Absatz 3 BDSG-E gegenüber den in § 203 Absatz 1, 2 a und 3 StGB genannten Personen, überwiegend Berufsheimnisträger, und deren Auftragsverarbeitern eingeschränkt. Dies ist richtig, weil anderenfalls in das Vertrauensverhältnis eingegriffen würde, das z. B. dem Mandatsverhältnis bei Rechtsanwälten oder dem Patientenverhältnis bei Ärzten zugrunde liegt.

Im Rahmen von arbeitsgerichtlichen Verfahren sind nach § 11 Absatz 2 Nummer 4 ArbGG jedoch auch Vereinigungen von Arbeitgebern vertretungsbefugt. In der Praxis hat diese Art der Vertretung bei arbeitsrechtlichen Rechtsstreitigkeiten eine große Bedeutung. Die Vertraulichkeit muss daher auch in diesem Verhältnis geschützt werden, so dass eine Regelung aufgenommen werden sollte, mit der die Betroffenenrechte und die Befugnisse der Aufsichtsbehörden auch in den Bevollmächtigtenverhältnissen nach § 11 Absatz 2 Nummer 4 ArbGG zurücktreten.

5. Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften, § 31 BDSG-E

Der HDE hatte in seiner Stellungnahme zum Referentenentwurf die bisher beabsichtigte Übernahme der Regelungen der §§ 28 a, 28 b BDSG in das novellierte Bundesdatenschutzgesetz begrüßt und auf die Vorteile des Kaufs auf Rechnung für den Verbraucher hingewiesen. Gleichzeitig muss der Händler jedoch das Risiko eines Zahlungsausfalls beurteilen können, wenn er seine Waren an den Verbraucher versendet, ohne gleichzeitig den vereinbarten Kaufpreis zu erhalten.

Die Regelung des neuen § 31 Absatz 2 Satz 1 BDSG-E lehnen wir jedoch entschieden ab.

a) Verlagerung der Verantwortung auf den Kunden der Auskunftfei

Anstelle der Übermittlung von Daten an Auskunftfeien nach § 28 a BDSG soll danach künftig die Verwendung der Daten durch den Kunden der Auskunftfei (z. B. den Online-Händler) geregelt werden. Dabei sollen die gleichen Voraussetzungen gelten wie bisher für die Übermittlung von Daten *an* die Auskunftfei. Derjenige, der



bei einer Auskunft eine Wahrscheinlichkeitswert über die Zahlungsfähigkeit bzw. -willigkeit abfragt, würde danach dafür verantwortlich sein, dass die ursprüngliche Einmeldung der Daten an die Auskunft unter den Voraussetzungen des bisherigen § 28 a BDSG erfolgt ist und die Datenverarbeitung bei der Auskunft datenschutzrechtskonform war. Der Bundesrat hat dieses Problem offensichtlich auch erkannt (Ziffer 36 der Stellungnahme, BR-Drs. 110/17(B)). Die von ihm in Ziffer 36 der Stellungnahme vorgeschlagene Ergänzung führt jedoch nicht zu einer Lösung des Problems.

Diese Verlagerung der Verantwortung auf den Online-Handel als einem der großen Kunden von Auskunftseien lehnen wir ab. Der Online-Händler, der lediglich das Ergebnis der Bewertung der Kreditwürdigkeit des Kunden erhält, kann weder überprüfen, ob die Daten rechtskonform an die Auskunft übermittelt worden sind, weil er nicht weiß, wer wann welche Daten übermittelt hat und welche Schritte dem vorausgegangen sind. Noch kann er prüfen, wie das Ergebnis durch die Auskunft zustande gekommen ist. Es ist auch nicht seine Aufgabe, deren Verantwortung für Einhaltung der datenschutzrechtlichen Vorgaben bei der Bildung des Scorewertes zu übernehmen. Rechtssicherheit würde nur durch eine Übernahme der bisherigen Regelungen der §§ 28 a und b BDSG geschaffen, nicht aber durch die nun von der Bundesregierung vorgelegte Regelung. Richtig ist daher der vom Bundesrat in Ziffer 38 der Stellungnahme vorgeschlagene Ansatz, wieder an die Datenübermittlung an Auskunftseien anzuknüpfen. Dies sollte aber an Stelle der Regelung des § 31 Absatz 2 Satz 1 und nicht ergänzend geschehen.

Die in Ziffer 33 d) der Stellungnahme des Bundesrats geforderte Erweiterung des Bußgeldkatalogs auf Verstöße gegen die Regelungen des § 31 BDSG-E ist dagegen – zumindest bezogen auf die aktuell vorliegende Regelung des Gesetzentwurfs – völlig verfehlt. Auch Ordnungswidrigkeitentatbestände müssen schon aus rechtsstaatlichen Erwägungen an ein vorwerfbares Verhalten anknüpfen. Dies dürfte kaum vorliegen, wenn der Verwender eines Scorewertes keinerlei Einfluss auf dessen Zustandekommen hat.

b) Erfüllung der Voraussetzungen des § 31 Absatz 2 Satz 1 BDSG-E durch einen Dritten

Nach § 31 Absatz 2 Satz 1 Nummer 4 c) wird für eine Einbeziehung von Forderungsausfällen in die Ermittlung eines Wahrscheinlichkeitswertes u. a. vorausgesetzt, dass der Gläubiger den Schuldner zuvor, jedoch frühestens bei der ersten Mahnung, über eine mögliche Berücksichtigung durch eine Auskunft unterrichtet hat. Ungeachtet der oben behandelten Frage, wer für die Einhaltung der Voraussetzungen der Übermittlung an die Auskunft verantwortlich sein soll, sollten die Voraussetzungen § 31 Absatz 2 Satz 1 Nummer 4 c) BDSG-E nicht nur durch eine Information des Gläubigers selbst, sondern auch durch einen Dritten, z. B. eines Inkassounternehmens, erfüllt werden können. Wir schlagen für § 31 Absatz 2 Satz 1 Nummer 4 c) BDSG-E daher folgende Formulierung vor:

„c) der Schuldner zuvor, jedoch frühestens bei der ersten Mahnung, über eine mögliche Berücksichtigung durch eine Auskunft informiert worden ist und“



6. Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person, § 32 BDSG-E

Die Einschränkungen der Informationspflicht im Zusammenhang mit der zweckändernden Datenverarbeitung, insbesondere bei einem unverhältnismäßigen Aufwand, werden begrüßt. Die erhebliche Ausweitung der Informationspflichten durch die Datenschutzgrundverordnung führt zu einem stark steigenden Aufwand der Unternehmen. Es ist daher richtig, zumindest in den Fällen die Pflicht zur Information des Betroffenen entfallen zu lassen, wenn dies mit einem unverhältnismäßigen Aufwand verbunden wäre oder sich als unmöglich erweist.

7. Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, § 33 BDSG-E

§ 33 BDSG-E ergänzt die Ausnahmen von der Informationspflicht gegenüber dem Betroffenen, wenn die Daten nicht bei ihm erhoben worden sind. Richtig ist, dass auch insoweit mehrere Regelungen des geltenden Bundesdatenschutzgesetzes in den Referentenentwurf aufgenommen worden sind, soweit die Verordnung dies ermöglicht.

Aus Sicht des HDE sollte § 33 Abs. 2 S. 1 Nr. 7 Buchstabe a) BDSG jedoch auch ausdrücklich in den Gesetzestext übernommen werden. Derzeit wird lediglich im Begründungstext zu § 32 BDSG-E (S. 106 unten) unter Bezugnahme auf § 33 Abs. 2 S. 1 Nr. 7 Buchstabe a) BDSG-E darauf hingewiesen, dass sich eine Unverhältnismäßigkeit auch aus der Zahl der betroffenen Personen ergeben könne. Dies ist für unter dem Gesichtspunkt der Praktikabilität nicht ausreichend. Aus Sicht des HDE wäre eine klarere Regelung vorzugswürdig, um die Möglichkeit, Daten aus öffentlich zugänglichen Quellen zu erheben und zu verarbeiten, auch tatsächlich weiter nutzen zu können. Es ist auch zu berücksichtigen, dass bei öffentlich zugänglichen Daten, die der Betroffene meist selbst veröffentlicht hat oder der Veröffentlichung zugestimmt hat, das Interesse an einer Information über die Datenerhebung in der Regel nicht oder nur sehr eingeschränkt vorhanden sein dürfte.

8. Datenschutzbeauftragte nicht-öffentlicher Stellen (§ 38 BDSG-E)

In § 38 BDSG-E wird Artikel 37 Absatz 1 DSGVO dahingehend konkretisiert, dass die Bestellung eines Datenschutzbeauftragten bereits erforderlich ist, wenn mindestens zehn Beschäftigte ständig mit der automatisierten Beschäftigung von Daten befasst sind. Damit soll die heutige Rechtslage übernommen werden.

Aus Sicht des HDE sollte das Gesetzgebungsverfahren zum Anlass genommen werden, die Voraussetzungen für die Bestellung eines Datenschutzbeauftragten an die technischen Entwicklungen von Betrieben anzupassen. Angesichts der Digitalisierung ist die Beibehaltung eines Schwellenwertes von zehn Mitarbeitern, die ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind, nicht mehr zeitgemäß. Dieser Schwellenwert sollte daher angehoben werden, um mittelständische Einzelhändler von der Verpflichtung zur Bestellung eines internen oder externen Datenschutzbeauftragten zu entlasten. Dies ist gerade im grenzüberschreitenden Online-Handel für die Wettbewerbsfähigkeit deutscher Anbieter von Bedeutung, weil es in anderen Mitgliedstaaten eine entsprechende Verpflichtung nicht gibt.



Fazit

Der HDE begrüßt, dass das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 noch in dieser Legislaturperiode verabschiedet werden soll. Zusammenfassend sollten nach Auffassung des HDE folgende Aspekte im weiteren Gesetzgebungsverfahren besonders berücksichtigt werden:

- Die Übernahme des § 6 b BDSG in den § 4 BDSG-E ist unter dem Gesichtspunkt der Rechtssicherheit im Moment praktikabel. Angesichts der restriktiven Auslegungspraxis durch die Aufsichtsbehörden wird aber darauf hingewiesen, dass die nationale Regelung im nicht-öffentlichen Bereich keine Einschränkung der Grundverordnung herbeiführen darf und zu beobachten ist, ob die Datenschutzgrundverordnung künftig eine großzügigere Praxis zulassen wird.
- Die vom Bundesrat vorgeschlagene Regelung des § 4 Absatz 5 Satz 2 BDSG-E, nach der die Löschung von Videoaufzeichnungen innerhalb von sieben Werktagen stets als unverzüglich gilt, sollte nicht nur für die Fälle des § 4 Absatz 1 Satz 2 BDSG-E, sondern für die Videoüberwachung generell gelten.
- Die Aufzählung des § 4 Absatz 1 Satz 2 Nr.1 BDSG-E sollte auch die Einzelhandelsgeschäfte mit einbeziehen.
- § 4 Abs. 2 BDSG-E sollte eine allgemeine Kennzeichnungsvorschrift für die Videoüberwachung beinhalten, die der heutigen Rechtslage des § 6 b Abs. 2 BDSG entspricht. Insbesondere sollte die Pflicht entfallen, die Videoüberwachung zum frühestmöglichen Zeitpunkt erkennbar zu machen. Dadurch würde die Information für die Betroffenen verschlechtert, weil dann nicht mehr genau abzugrenzen ist, in welchem Bereich tatsächlich eine Videoüberwachung stattfindet.
- Die Regelungen zur zweckändernden Datenverarbeitung für nicht öffentliche Stellen nach § 24 Abs. 1 BDSG-E sollten wieder die Befugnis zur zweckändernden Datenverarbeitung aufgrund eines berechtigten Interesses beinhalten, wie es bereits im Referentenentwurf vorgesehen war. Keinesfalls dürfen weitere Einschränkungen erfolgen, wie es der Bundesrat fordert.
- Bei der Datenverarbeitung im Beschäftigtenkontext nach § 26 BDSG-E ist die Definition der Kollektivvereinbarung zu begrüßen. Die zusätzlichen Anforderungen an die Einwilligung sollten gestrichen und die Einbeziehung des von Zeitarbeitnehmern in den Beschäftigtenbegriff gegenüber dem Entleiher entfallen. Sollte entgegen der Ansicht des HDE an der Regelung im Grundsatz festgehalten werden, muss aus Sicht des HDE zumindest das Schriftformerfordernis für die Einwilligung auf die Textform nach § 126 b BGB reduziert werden.
- Der Schutz von geheimhaltungsbedürftigen Informationen nach § 29 BDSG-E sollte auch auf die im arbeitsgerichtlichen Verfahren vertretungsbefugten Arbeitgeberverbände und Gewerkschaften nach § 11 Absatz 2 Nummer 4 ArbGG ausgeweitet werden, weil insoweit ein einem rechtsanwaltlichen Mandatsverhältnis entsprechendes Vertrauensverhältnis besteht.
- Im Zusammenhang mit der Neuregelung des Scorings wird in § 31 Absatz 2 Satz 1 BDSG-E als besonders problematisch abgesehen, dass das Anknüpfen an die Verwendung der Auskunft zu einer Verlagerung der Verantwortlichkeit auf die Kunden der Auskunfteien führt. Diese können aber weder die Rechtmäßigkeit der Einmeldungen noch die Rechtmäßigkeit der Datenverarbeitung bei der Auskunftei kontrollieren. Es sollte wie bisher an die Übermittlung von Daten an die Auskunftei angeknüpft werden. Die vom Bundesrat geforderten Gesetzesverschärfungen lehnen wir ab.
- Die Regelung des § 33 Abs. 2 S. 1 Nr. 7 Buchstabe a) BDSG, nach der eine Pflicht zur Benachrichtigung der betroffenen Person nicht besteht, wenn die Daten für eigene Zwecke gespeichert sind, sie aus allge-



mein zugänglichen Quellen entnommen worden sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist, sollte ergänzend in § 33 BDSG-E aufgenommen werden.

- Der Schwellenwert für die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten nach § 38 BDSG-E sollte angehoben werden.