Betrug im Onlinehandel nicht Tür und Tor öffnen

Positionspapier zum Kabinettsbeschluss zum 1. BDSGÄndG

13. März 2024

Der Entwurf zur Änderung des BDSG beinhaltet neben neuen Regelungen zur Datenschutzkonferenz (DSK) unter anderem auch Änderungen, die vermutlich darauf abzielen, Zahlungsfähigkeitsdiskriminierung abzustellen. Leider ist dabei jedoch der Anwendungsbereich so weit gefasst, dass durch die vorgeschlagenen Regelungen die Betrugsprävention stark eingeschränkt werden würde.

Betrugsprävention ist im Onlinehandel von großer Bedeutung

Durch eine wirksame Betrugsprävention werden Verbraucher*innen vor Identitätsdiebstahl, betrügerischen Transaktionen und finanziellen Verlusten geschützt. Dies trägt dazu bei, das Vertrauen der Verbraucher*innen in den Onlinehandel aufrechtzuerhalten und ihre Sicherheit beim Einkaufen im Internet zu gewährleisten.

Betrug im Onlinehandel kann erhebliche wirtschaftliche Schäden für Unternehmen verursachen, sei es durch finanzielle Verluste, Rückbuchungen von Zahlungen oder die Beeinträchtigung des Markenrufs. Eine wirksame Betrugsprävention hilft Unternehmen, diese Risiken zu minimieren und ihre wirtschaftliche Stabilität zu erhalten.

Betrug kann nicht nur finanzielle Verluste für Verbraucher*innen verursachen, sondern auch den Ruf von Onlinehändlern und den der gesamten Branche beeinträchtigen. Durch die Vermeidung von Betrug wird die Integrität des Onlinehandels gewahrt und ein positives Geschäftsumfeld geschaffen.

Ein sicherer und vertrauenswürdiger Onlinehandel fördert das Wachstum der Branche, indem er Verbraucher*innen dazu ermutigt, online einzukaufen und Unternehmen dazu ermutigt, in den Onlinevertrieb zu investieren. Eine effektive Betrugsprävention schafft ein Umfeld, das das Wachstum und die Innovation im Onlinehandel unterstützt.

Letztlich sind Unternehmen im Onlinehandel sogar gesetzlich dazu verpflichtet, angemessene Maßnahmen zur Betrugsprävention zu ergreifen und die Sicherheit ihrer Kunden*innen zu gewährleisten. Die DSGVO erkennt die Betrugsprävention daher ausdrücklich als Grund (legitimes Interesse) für Datenverarbeitung an.

Denn Betrugsprävention im Onlinehandel ist entscheidend, um Verbraucher*innen zu schützen, das Vertrauen in den Onlinehandel aufrechtzuerhalten, wirtschaftliche Schäden zu vermeiden und das Wachstum der Branche zu fördern.

Rechtssicherheit ist gerade im Datenschutzbereich besonders wichtig

Rechtssicherheit ist ein entscheidender Aspekt für Unternehmen, da sie eine stabile Grundlage für Geschäftsaktivitäten bietet und das Risiko rechtlicher Unsicherheiten und potenzieller Streitigkeiten minimiert. Insbesondere im Bereich des Datenschutzes ist Rechtssicherheit von großer Bedeutung, da dieser Bereich häufig von divergierenden Auslegungen und Interpretationen geprägt ist, was zu einer erhöhten Rechtsunsicherheit führt.

Die Einführung neuer Klageinstrumente und die verstärkte Überwachung von Unternehmen im Datenschutzbereich sind grundsätzlich zu begrüßen, da sie den Schutz der Privatsphäre und der Daten der Verbraucher*innen fördern. Jedoch wird dadurch auch die Notwendigkeit klarer und eindeutiger Formulierungen in den Gesetzen noch dringlicher. Unternehmen müssen in der Lage sein, die Anforderungen des Datenschutzrechts eindeutig zu verstehen und entsprechende Maßnahmen zu ergreifen, um ihre Datenverarbeitungen in Einklang mit den gesetzlichen Vorgaben zu bringen.

Rechtsunsicherheit im Bereich des Datenschutzes kann erhebliche zusätzliche Kosten verursachen, aber auch Innovation behindern, da Unternehmen möglicherweise zögerlich sind, neue Technologien und datenbasierte Produkte zu entwickeln.

§ 37a BDSGÄndG-E ist inhaltlich und handwerklich nicht geglückt

Der Entwurf einer Regelung in § 37a BDSG-E ist aus unserer Sicht inhaltlich und auch handwerklich nicht geglückt. Bei einer falschen Lesart der Vorschrift könnte diese erhebliche negative Auswirkungen auf Onlinehändler haben und auch dem Bedürfnis des Schutzes der Verbraucher*innen zuwiderlaufen. Im Einzelnen:

A. Der EUGH hat die vorgeschlagenen Änderungen gar nicht verlangt

Nach unserem Verständnis basiert der Vorschlag auf dem Umstand, dass der EuGH in dem Verfahren „SCHUFA / automatisierte Einzelfallentscheidung“ einen Hinweis dahingehend gegeben hat, dass die jetzige Vorschrift in § 31 Abs.1 BDSG nicht europarechtskonform sei. Wir nehmen daher an, dass mit der vorgeschlagenen Änderung eine gesetzliche Regelung für die Datenverarbeitungen durch Auskunfteien geschaffen werden soll.

Das hat der EUGH allerdings überhaupt nicht verlangt. Der Europäische Gerichtshof hat festgestellt, dass die SCHUFA in bestimmten Situationen automatisierte Einzelentscheidungen trifft, die sich auf Betroffene auswirken, wenn sie von Dritten (z.B. Händlern) verwendet werden ohne dass die Händler die näheren Umstände dieser Entscheidung steuern oder kontrollieren können. Dies ließ eine Schutzlücke bei den Auskunftsansprüchen entstehen, welche der EuGH nunmehr schließen wollte. Ohne das Vorliegen einer automatisierten Einzelfallentscheidung hätte eine betroffene Person kein Recht darauf, von der SCHUFA Auskunft über ihre Scorewertbildung zu erhalten, wie es in Art. 15 Abs. 1 Ziffer h) der DSGVO vorgesehen ist.

Damit hat der EuGH zur Schließung einer Schutzlücke die automatisierte Einzelfallentscheidung zeitlich auf die Auskunftei vorverlagert. Dogmatisch konsequent muss daher auch die im Massenverkehr (z. B. Onlinehandel) einschlägige Ausnahmeregelung in Art. 22 Abs.2 Ziffer a) DSGVO vorverlegt gelten und der Auskunftei eine vollautomatisierte Entscheidung erlaubt bleiben, wenn diese vor dem Hintergrund eines Vertragsabschlusses eines Händlers erfolgt.

Der Entscheidung des EuGH ist nicht zu entnehmen, dass der Anwendungsbereich des Art. 22 DSGVO nicht ganzheitlich auf Auskunfteien ausgedehnt oder etwa im Regelungsbereich aufgespalten werden sollte. Der Entwurf des § 37a BDSG-E führt jedoch zu eben jener Aufspaltung. Diese ist weder von der DSGVO gedeckt noch vom EuGH vorgesehen, woraus sich die Europarechtswidrigkeit ergibt.

B. Änderungen müssen auf die richtige Öffnungsklausel gestützt und auf Auskunfteien beschränkt werden

In dem Entwurf wird die nationale Gesetzgebungskompetenz auf die Öffnungsklausel in Art. 22 Abs.2 Ziffer b) DSGVO gestützt. Diese ist aber sehr „eng“, da sie ausschließlich die automatisierte Einzelfallentscheidung an sich erfasst. Vor diesem Hintergrund bestehen erhebliche Zweifel, ob die Öffnungsklausel für die geplante Änderung verwendet werden darf. Dies gilt insbesondere für die einzuhaltenden „materiellrechtlichen“ Voraussetzungen (z.B. keine Nutzung von Anschriftendaten). Diese materiellrechtlichen Voraussetzungen sollen wohl eine Ausformung der „*angemessenen Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person*“ (Art. 22 Abs.2 Ziffer b) DSGVO) darstellen. Bei den in Art. 22 Abs.2 Ziffer b) DSGVO genannten Maßnahmen kann es sich aber lediglich um „verfahrensrechtliche“ handeln, was sich bereits aus den Vorgaben aus Art. 22 Abs.3 DSGVO ergibt. Nach der Rechtsprechung des EuGH sind materiellrechtliche Vorgaben stets anhand der Vorschrift Art. 6 DSGVO zu messen.

Besser wäre es aus unserer Sicht, eine Regelung – sofern man diese überhaupt schaffen möchte – auf die Öffnungsklausel in Art. 23 Abs.1 Ziffer e) DSGVO (allgemeines öffentliches Interesse) zu stützen. Dies kann aus unserer Sicht rechtssicher erfolgen, wenn man den § 37a BDSG auf die Datenverarbeitung durch Auskunfteien beschränkt. Hierfür müsste unter anderem die Regelung in § 37a Abs.1 Nr.1 BDSG-E gestrichen werden. Dies wäre logisch konsequent, da im EuGH-Urteil in erster Linie um Datenverarbeitungen durch Auskunfteien geregelt werden.

C. § 37a Abs.2 BDSG-E muss die Ausnahmetatbestände klar benennen

Die Vorschrift in § 37a Abs.2 BDSG-E ist von ihrem Wortlaut her nicht eindeutig so zu verstehen, dass diese keine Anwendung findet, wenn Verantwortliche sich auf die Ausnahmetatbestände in Art. 22 Abs.2 Ziffer a) und c) DSGVO berufen können. Die Begründung in dem Entwurf ist zwar wohl dahingehend zu verstehen – die Regelung muss aber eindeutig formuliert sein, um in diesem zentralen Punkt Rechtssicherheit und präzise Anwendungsklarheit zu schaffen.

D. Anschriftendaten müssen für die Betrugsprävention genutzt werden dürfen

Die Nutzung von Anschriftendaten ist im Rahmen der Betrugsprävention essentiell. Es gibt nämlich z.B. anonyme Anschriften (große Wohnblöcke, öffentliche Einrichtungen, etc.), die es Betrügern leichter machen, Bestellbetrug zu begehen.
Dass diese Daten im Rahmen der Betrugsprävention bzw. bei der Bildung von Betrugsscores genutzt werden dürfen, haben die Datenschutzbehörden anerkannt. Die Schaffung von Lücken im Bereich der Betrugsprävention läuft auch den Verbraucher*inneninteressen zuwider. Versandhändler sind im Übrigen bereits aus gesetzlichen Gründen dazu verpflichtet, Identitätsdiebstähle zu vermeiden. Dies ergibt sich aus der Entscheidung des BGH „Identitätsdiebstahl II“. Hierfür müssen sie die relevanten Daten, zu denen insbesondere auch Anschriftendaten gehören, verarbeiten dürfen. Darüber hinaus steht die Regelung auch im Widerspruch dazu, dass der Europäische Gesetzgeber im Rahmen der KI-Verordnung ausdrücklich festgelegt hat, dass der Einsatz von KI zum Zweck der Betrugsprävention nicht unter die Kategorie „Hochrisiko“ fällt.

E. Zweckbegrenzung ist europarechtswidrig

Die Zweckbegrenzung in § 37a Abs.2 Nr.3 b) BDSG-E ist nicht mit den Grundsätzen aus Art. 6 Abs.4 DSGVO vereinbar. In der Praxis werden dieselben Datenkategorien vollkommen rechtmäßig für eine Vielzahl an Zwecken genutzt.

F. Geschäftsgeheimnisse werden zu weitreichend eingeschränkt

§ 37a Abs.6 BDSG-E soll sich vermutlich auf die Bildung von Scorewerten beziehen. In der aktuellen Formulierung bezieht es sich aber auf die “Verantwortlichen”. Das bedeutet, dass dieser Absatz auch in anderen Fällen – die keine Scorewertbildung sind – Anwendung finden würde, solange der Verantwortliche auch Scorewerte bildet. Ein Unternehmen, das Scorewerte bildet, dürfte sich daher auch in anderen Fällen nicht auf die angedachte Ausnahme für den Schutz von Geschäftsgeheimnissen beziehen. Diese referenziert nämlich auf den Verantwortlichen, der Scorewerte bildet und nicht auf die Scorewertbildung an sich.

Was geändert werden muss:

- Den neuen § 37a auf Auskunfteien beschränken und § 37a Abs.1 Nr.1 BDSG-E streichen.
- § 37a Abs.2 BDSG-E eindeutig formulieren, damit sich Verantwortliche auf die Ausnahmetatbestände in Art. 22 Abs. 2 a) und c) DSGVO berufen können.
- Die Nutzung von Daten – insbesondere Anschriftendaten – für die Betrugsprävention weiter zulassen.
- Zweckbegrenzung in § 37a Abs. 2 Nr.3 b) BDSG-E streichen.
- § 37a Abs 6 BDSG-E umformulieren und auf die Bildung von Scorewerten beziehen.

Zur Otto Group
1949 in Deutschland gegründet, ist die Otto Group heute als weltweit agierende Handels- und Dienstleistungsgruppe mit rund 41.000 Mitarbeiter*innen in 30 wesentlichen Unternehmensgruppen vornehmlich in den drei Wirtschaftsräumen Deutschland, übriges Europa und USA präsent. Ihre Geschäftstätigkeit erstreckt sich auf die Segmente Plattformen, Markenkonzepte, Händler, Services und Finanzdienstleistungen. Eine Vielzahl von strategischen Partnerschaften und Joint Ventures bieten der Otto Group ausgezeichnete Voraussetzungen für Know-how-Transfer und die Nutzung von Synergiepotenzialen. Ein hohes Maß an unternehmerischer Verantwortung und Kollaborationswillen der Konzerngesellschaften garantieren zugleich Flexibilität und Kund*innennähe sowie eine optimale Zielgruppenansprache in den jeweiligen Ländern.

Zu Zalando
Zalando ist eine der führenden Online-Destinationen für Mode und Lifestyle in Europa. Im Jahr 2008 in Berlin gegründet, bietet Zalando heute mehr als 50 Millionen aktiven Kund*innen in 25 Ländern Produkte aus den Bereichen Bekleidung, Schuhe, Accessoires und Kosmetik. Als Europas modischstes Tech-Unternehmen suchen wir laufend nach neuen digitalen Lösungen für jeden Teil des Einkaufserlebnisses – für unsere Kund*innen, Partner*innen und alle anderen Akteure, die Zalando mit uns gestalten wollen. Unsere Vision ist, der Starting Point for Fashion – die erste Anlaufstelle für Mode – zu sein.