bitkom

Stellungnahme

Februar 2026

Bitkom zur Formulierungshilfe für die Fraktionen CDU/CSU und SPD zum Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2023/2225 über Verbraucherkreditverträge

Einordnung und Überblick

Bitkom begrüßt weiterhin das Ziel des Gesetzgebers, mit § 37a BDSG Rechtssicherheit im Anschluss an das Urteil des Europäischen Gerichtshofs vom 7. Dezember 2023 (C-634/21 – SCHUFA) zu schaffen.[1] Die nun vorliegende Formulierungshilfe stellt zwar gegenüber dem bisherigen Referentenentwurf eine Konkretisierung dar, wirft jedoch weiterhin rechtliche sowie praktische Fragen auf und verfehlt ihr Ziel Rechtssicherheit zu schaffen.

Aus Sicht des Bitkom ist insbesondere das ausnahmslose Verbot der Nutzung von Anschriftendaten und Kontodaten problematisch. In der vorliegenden Form gefährdet § 37a BDSG-neu nicht nur etablierte und anerkannte Verfahren der Betrugsprävention, sondern läuft auch Verbraucherinteressen zuwider.

[1] Stellungnahme des Bitkom »Datenverarbeitung für Scoring-Zwecke (§37a BDSG-E, »Scoring«), Mai 2024

Der EuGH-Entscheidung lag ausschließlich das externe Scoring durch Auskunfteien zugrunde. Eine darüberhinausgehende Ausweitung ist weder erforderlich noch begründbar.

Verwendung von Anschriftendaten

Die Formulierungshilfe sieht in § 37a Abs. 2 Nr. 1 lit. d) BDSG-neu ein ausnahmsloses Verbot der Nutzung von Anschriftendaten für die Erstellung und Verwendung von Wahrscheinlichkeitswerten vor. Diese Regelung geht deutlich über das hinaus, was durch das EuGH-Urteil veranlasst ist.

1. **Zentrale Bedeutung von Anschriftendaten im Risikosteuerungsprozess gegen Zahlungsausfälle und zur Ermöglichung von digitalen Geschäftsabschlüssen**

Anschriftendaten sind ein unverzichtbarer Bestandteil zur Absicherung gegen Zahlungsausfälle, z.B. durch betrügerisches Verhalten, sowohl im Online- und Versandhandel wie auch im Kredit- und Zahlungsverkehr. Bestimmte Anschriften (z. B. große Wohnanlagen, Sammeladressen oder öffentliche Einrichtungen) werden nachweislich überproportional häufig für Bestell- und Identitätsbetrug genutzt. Die Berücksichtigung solcher Muster dient nicht der Diskriminierung, sondern der Erkennung betrügerischer Konstellationen und damit der Vermeidung von Zahlungsausfällen und Preissteigerungen zulasten aller Verbraucherinnen und Verbraucher.

Deutsche Datenschutzaufsichtsbehörden haben die Nutzung von Anschriftendaten zu Zwecken der Betrugsprävention bislang ausdrücklich als zulässig anerkannt. Zudem sind Unternehmen – etwa Versandhändler – rechtlich verpflichtet, geeignete Maßnahmen zur Verhinderung von Identitätsdiebstahl zu ergreifen. Auch Zahlungs- und Kreditinstitute unterliegen nach PSD2 und ZAG expliziten Verpflichtungen zur Implementierung wirksamer Sicherheits- und Betrugspräventionsmaßnahmen. Diese Pflichten sind nicht fakultativ, sondern aufsichtsrechtlich durchsetzbar und geboten. Ein gesetzliches Verbot der Nutzung zentraler Risikomerkmale kann damit in einen strukturellen Konflikt zwischen Datenschutzrecht und Aufsichtsrecht führen. Unternehmen würden faktisch gezwungen, regulatorische Präventionspflichten mit reduzierten oder qualitativ geschwächten Modellen zu erfüllen.

Adressdaten sind nicht lediglich ergänzende Merkmale, sondern zentral für die Modellierung von Identity Takeover beim Kreditantrag (z. B. Social Engineering) sowie die Plausibilisierung transaktionsbezogener Auffälligkeiten (z. B. atypische geografische Nutzungsmuster). Ein pauschaler Ausschluss solcher Daten würde die Effektivität bestehender, aufsichtsrechtlich eingebetteter Fraud-Systeme erheblich beeinträchtigen und unterläuft die oben angesprochenen Pflichten.

Datenverarbeitung, die Verbraucher betrifft, soll zu richtigen und guten Entscheidungen führen und insbesondere nicht diskriminieren. Ein wesentlicher Baustein zur Sicherstellung dieser Ziele ist in Erwägungsgrund 71 Satz 6 der DSGVO enthalten. Danach müssen die für die Verarbeitung Verantwortlichen geeignete mathematische oder statistische Verfahren für ein Profiling verwenden. Maßgeblich für die Verarbeitung von Daten in diesem Kontext ist daher zunächst deren statistische

Relevanz für den zu ermittelnden Wahrscheinlichkeitswert. Sofern ein Datum keine statistische Relevanz für einen Wahrscheinlichkeitswert aufweist, entfällt auch die Rechtsgrundlage für die Verarbeitung. Schließt man andererseits aber von vornherein statistisch relevante Daten für die Ermittlung einer Wahrscheinlichkeit aus, kann dies bei fehlender Kompensationsmöglichkeit durch andere Daten, zu qualitativ schlechteren Ergebnisses führen.

Regelmäßig dürfte also die Berücksichtigung von Daten, die nach mathematisch statistischen Verfahren geeignet sind, auch zu besseren Entscheidungen oder Wertungen führen. Damit erscheint der pauschale Ausschluss von Datenkategorien, die statistisch mathematisch relevant sein können, nicht per se geeignet, den Verbraucherschutz zu erhöhen.

Zudem bieten die Regelungen der Art. 12 ff DSGVO zur Transparenz, insbesondere Art. 15 Abs. 1h DSGVO und das Recht auf Einwirkung des Eingreifens einer Person sowie der Darlegung des eigenen Standpunkts und der Anfechtung gemäß Art. 22 Abs. 3 DSGVO weiteren Schutz.

Bei einer Konzentration auf die Risikobewertung im Kreditwürdigkeitsprozess zeigt sich dies besonders deutlich: Die Risikobewertung umfasst regelmäßig auch Maßnahmen zur Absicherung gegen betrügerisches Verhalten, insbesondere im Online- und Versandhandel und ist gemäß Erwägungsgrund 47 Satz 6 DSGVO ausdrücklich als berechtigtes Interesse anerkannt. Bestimmte Anschriften (z. B. große Wohnanlagen, Sammeladressen oder öffentliche Einrichtungen) werden nachweislich überproportional häufig für Bestell- und Identitätsbetrug genutzt. Die Berücksichtigung solcher Muster dient nicht der Diskriminierung, sondern der Erkennung betrügerischer Konstellationen und damit der Vermeidung von Zahlungsausfällen und Preissteigerungen zulasten aller Verbraucherinnen und Verbraucher.

Mit der Formulierungshilfe wird der Katalog der unzulässigen Datenarten – auch zum Zwecke der Betrugsprävention um Kontodaten, Alter und Geschlecht erweitert. Diese pauschale Erweiterung verschärft die Problematik erheblich.

Alter und Geschlecht können – insbesondere im Kontext der Betrugsprävention – als technische Plausibilitäts- und Inkonsistenzmerkmale dienen (z. B. bei Aufdeckung von Identitätsmissbrauch), ohne dass sie zu einer diskriminierenden Bewertung führen. Ein ausnahmsloses gesetzliches Verbot verkennt diese Funktion und erschwert die Aufdeckung betrügerischer Sachverhalte erheblich.

Unter Berücksichtigung der vorstehenden Ausführungen regen wir an, die bisherige Regelung aus § 31 BDSG zu übernehmen und § 37a BDSG-E wie folgt zu ändern:

In Abs. 2 Nummer 1 Buchstabe d) wird das Wort »ausschließlich« hinzugefügt, so dass der Text dann lautet: (2) Wahrscheinlichkeitswerte im Sinne des Absatzes 1 dürfen nur erstellt oder verwendet werden, wenn 1. für die Erstellung folgende Daten nicht genutzt werden a) […] […] d) *ausschließlich* Anschriftendaten.

Die bisherige Regelung hat sich bewährt. Die Verschärfung in der Formulierungshilfe hinsichtlich eines Totalverbots der Nutzung von Anschriftendaten ist nicht auf konkrete Anlässe einer Benachteiligung bestimmter Wohngegenden zurückzuführen.

2. **Verbraucherschutz und Systemvertrauen**

Eine Einschränkung effektiver Betrugsprävention schadet nicht nur Unternehmen, sondern unmittelbar auch Verbraucherinnen und Verbrauchern. Funktionierende Fraud-Scoring-Verfahren schützen vor finanziellen Schäden, Identitätsmissbrauch und Vertrauensverlust in digitale Geschäftsmodelle. Die geplanten Verbote würden faktisch Betrug erleichtern und stehen damit im Widerspruch zu den Zielen der Verbraucherkreditrichtlinie und des Verbraucherschutzes insgesamt. .

3. **Unverhältnismäßigkeit des Totalverbots**

Statt eines ausnahmslosen Verbots wäre eine differenzierende Regelung erforderlich. Maßgeblich muss allein sein, dass die jeweilige Datenverarbeitung den Anforderungen des Art. 6 DSGVO genügt.

Die Interessen der Betroffenen werden ausreichend geschützt. Die Entscheidung des EuGH vom 27.02.25 (C-203/22) gibt den Betroffenen umfangreiche Auskunftsrechte.

Der Gesetzgeber darf keine zusätzlichen materiellen Voraussetzungen für bestimmte Datenarten schaffen. Sollte gleichwohl an einer nationalen Regelung festgehalten werden, sollte die Nutzung von Anschriftendaten zumindest jedenfalls dann zulässig sein, wenn sie

- nicht ausschließlich,
- diskriminierungsfrei und
- nachweislich zur Risikominimierung eingesetzt werden. Gleiches gilt für Alter, Geschlecht und Informationen zu Kontodaten.

Rechtssicherheit schaffen: von der Datenschutzaufsicht genehmigte Verhaltensregeln gesetzlich verankern

Die Verbraucherkreditrichtlinie sieht für Verbraucherdarlehensverträge künftig eine verpflichtende, eingehende Kreditwürdigkeitsprüfung vor. Die praktische Umsetzung dieser Vorgabe ist aufgrund aktueller Rechtsprechung gefährdet und es besteht erhebliche Rechtsunsicherheit bei der Durchführung der Kreditwürdigkeitsprüfung. Wir benötigen dringend Rechtssicherheit bei der Erfüllung dieses gesetzlich vorgeschriebenen Prozesses im Risikomanagement. Dies ist auch mit Blick auf die Gewährleistung des nach der Verbraucherkreditrichtlinie verpflichteten Überschuldungsschutzes unabdingbar.

Die Verwendung statistisch relevanter Informationen aus einem begrenzten Kreis bonitätsrelevanter Daten, ist grundlegend für verlässliche Risikobewertungen. Gerichtsentscheidungen haben in der Vergangenheit die Speicherfristen für einzelne Datenarten (sog. erledigte Zahlungsstörungen), die im Rahmen der Kreditwürdigkeitsprüfung verwendet werden und im Code of Conduct Prüf- und Speicherfristen von personenbezogenen Daten geregelt sind, in Frage gestellt.

Der Bundesgerichtshof hat in seiner Entscheidung vom 18. Dezember 2025 die Prüf- und Speicherfristen des Code of Conduct, sowie die Wirkweise als typisierte Interessenabwägung bestätigt. Der Code of Conduct nimmt aus Sicht des Senats einen grundsätzlich angemessenen Interessenausgleich vor.

Umfängliche Rechtssicherheit für die grundsätzliche Verwendung bonitätsrelevanter Daten kann allerdings nur durch eine verlässliche Rechtsgrundlage geschaffen werden. Diese kann nur der Gesetzgeber schaffen.

Der Bitkom empfiehlt daher, im Rahmen der Einführung des § 37 a BDSG Rechtssicherheit für alle Beteiligten zu schaffen. Dies ist mit einer gesetzlichen Verankerung des jeweils aktuellen Code of Conducts einfach umzusetzen. Alle deutschen Datenschutzaufsichten haben die Speicherfristen des Code of Conducts bereits einstimmig genehmigt.

Anwendungsbereich des § 37a BDSG

Auch in der aktuellen Fassung bleibt problematisch, dass § 37a Abs. 1 Nr. 1 BDSG-neu den Anwendungsbereich weit über externes Scoring hinaus öffnet. Die Regelung erfasst potenziell jede Form der Wahrscheinlichkeitsbewertung im Rahmen vertraglicher Entscheidungen, ohne sachliche Differenzierung.

Dies schafft erhebliche Rechtsunsicherheit, ohne dass hierfür eine unionsrechtliche Notwendigkeit besteht.

Zweckbindung gemäß § 37a Abs. 2 Nr. 3 lit. b) BDSG

Die vorgesehene Zweckbindung, wonach für Scoring genutzte Daten »für keine anderen Zwecke« verarbeitet werden dürfen, ist weiterhin kritisch zu bewerten. Sie ergibt sich weder aus der EuGH-Rechtsprechung zu Art. 22 DSGVO noch ist sie mit Art. 6 Abs. 4 DSGVO vereinbar. Eine vergleichbare nationale Regelung existiert in keinem anderen EU-Mitgliedsstaat.

Damit werden deutsche Unternehmen erneut einseitig belastet. Bitkom empfiehlt die Streichung von § 37a Abs. 2 Nr. 3 lit. b) BDSG-neu.Zusammenfassung der Änderungsvorschläge

Bitkom spricht sich insbesondere für folgende Anpassungen aus:

- Streichung pauschaler Datenartenverbote ohne Differenzierung zu Möglichkeiten der Betrugsprävention.
- Gesetzliche Verankerung des jeweils geltenden Code of Conduct;
- Streichung der zusätzlichen Zweckbindung in § 37a Abs. 2 Nr. 3 lit. b) BDSG
- Klarstellung, dass legitime, Fraud-Risiko-Scoring-Verfahren weiterhin zulässig bleiben

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Isabelle Stroot | Bereichsleiterin Datenschutzrecht & -politik
T 030 27576-228 | i.stroot@bitkom.org

Alina Stephanie Bone-Winkel | Bereichsleiterin Digital Banking & Financial Services
T 0 30 27576-273 | a.bone-winkel@bitkom.org

Tim Haremsa | Referent Digital Banking & Financial Services
T 0 30 27576-429 | t.haremsa@bitkom.org

Verantwortliches Bitkom-Gremium

AK Datenschutz
AK FinTechs & Digital Banking
AK Digitaler Zahlungsverkehr