

# Stellungnahme

des Gesamtverbandes der  
Deutschen Versicherungswirtschaft  
Lobbyregister-Nr. R000774

zum Regierungsentwurf eines Ersten Gesetzes zur  
Änderung des Bundesdatenschutzgesetzes

## Inhalt

<b>1. § 37a RegE BDSG .....</b>	<b>2</b>
1.1 Informationen über Zahlungseingänge und -ausgänge auf und von Bankkonten (§ 37a Abs. 2 Nr. 1 Buchst. c) BDSG-RegE) .....	3
1.2 Keine anderen Zwecke (§ 37a Abs. 2 Nr. 3 Buchst. b) BDSG-RegE) .....	4
1.3 Keine unerlaubte Konkretisierung des Art. 6 DSGVO durch § 37a Abs. 2 BDSG-RegE .....	4
1.4 Schutz von Geschäftsgeheimnissen (§ 37a Abs. 5 BDSG-RegE) .....	5
<b>2. Vollautomatisierte Einzelentscheidungen zur Risiko- und Leistungsprüfung in der Versicherungswirtschaft (§ 37 BDSG) .....</b>	<b>5</b>
<b>3. Zuständigkeit der Datenschutzaufsichtsbehörden .....</b>	<b>6</b>
<b>4. Weitere Vorschläge .....</b>	<b>8</b>



**Gesamtverband der Deutschen Versicherungswirtschaft e. V.**  
Wilhelmstraße 43 / 43 G, 10117 Berlin  
Postfach 08 02 64, D-10002 Berlin  
Telefon: +49 30 2020-5000 · Telefax: +49 30 2020-6000  
Lobbyregister-Nr. R000774

**Ansprechpartner**  
Datenschutz/Grundsatzfragen

**E-Mail**  
[data-protection@gdv.de](mailto:data-protection@gdv.de)

Rue du Champ de Mars 23, B-1050 Brüssel  
Telefon: +32 2 28247-30 · Telefax: +49 30 2020-6140  
ID-Nummer 6437280268-55  
[www.gdv.de](http://www.gdv.de)

## Zusammenfassung

Die Streichung von § 31 BDSG und die Einfügung von § 37a BDSG-RegE sind wichtige Schritte, um nach dem Schufa-Urteil des EuGH wieder mehr Rechtssicherheit für die Erstellung und Verwendung von Wahrscheinlichkeitswerten zu schaffen. Allerdings sollten § 37a Abs. 2 Nr. 1 Buchst. c) und Nr. 3 Buchst. b) BDSG-RegE präziser gefasst werden, um keine ungewollten Auswirkungen zu haben (dazu Ziffer 1).

Die in § 37 BDSG geregelten Ausnahmen für vollautomatisierte Einzelentscheidungen sollten erweitert werden, um im Massengeschäft der Versicherer schnelle automatisierte Vertragsabschlüsse und Schadenregulierungen zu ermöglichen (dazu Ziffer 2).

Die Regelungen zur Zuständigkeit der Aufsichtsbehörden in § 27 Abs. 5 und § 40a BDSG-RegE sind ein guter Ansatz, um divergierende Entscheidungen unterschiedlicher Aufsichtsbehörden zu verhindern. § 40a BDSG-RegE sollte jedoch auf alle Datenverarbeitungen in Unternehmensgruppen ausgeweitet werden und mehr Flexibilität bei der Bestimmung der zuständigen Behörde gewähren (dazu Ziffer 3).

Weitere Anregungen enthält unsere Stellungnahme zum Referentenentwurf.

### 1. § 37a RegE BDSG

Mit der Streichung des § 31 BDSG und der Einfügung des neuen § 37a BDSG-RegE hat die Bundesregierung auf das Urteil des Europäischen Gerichtshofs vom 07.12.2023 in der Rechtssache C 634/21 (Schufa) reagiert. Dies ist nötig, um Rechtssicherheit für Auskunftfeien und ihre Kunden zu schaffen.

Die in § 37a Abs. 1 BDSG-RegE vorgesehene neue Ausnahme vom Verbot des Art. 22 Abs. 1 DSGVO kann für Versicherungsunternehmen zum einen als Verwender von Scorewerten, die sie von Auskunftfeien erhalten, relevant sein. § 37a Abs. 1 Nr. 1 BDSG-RegE kann aber auch einschlägig sein, wenn ein Versicherungsunternehmen selbst einen Wahrscheinlichkeitswert über ein zukünftiges Verhalten errechnet, um über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses zu entscheiden.

Allerdings sind einige Anforderungen des § 37a Abs. 2 und 5 BDSG-RegE für die Datenverarbeitung in den Versicherungsunternehmen zu eng und teilweise auch missverständlich.

### 1.1 Informationen über Zahlungseingänge und -ausgänge auf und von Bankkonten (§ 37a Abs. 2 Nr. 1 Buchst. c) BDSG-RegE)

§ 37a Abs. 2 Nr. 1 Buchst. c) BDSG-RegE legt fest, dass Wahrscheinlichkeitswerte im Sinne von § 37 Abs. 1 BDSG-RegE keine Informationen über Zahlungseingänge und -ausgänge auf und von Bankkonten enthalten dürfen. Ziel der Regelung ist es, zu vermeiden, dass „im großen Umfang Erkenntnisse über persönliche Aspekte der Lebensführung“ gewonnen und verwertet werden (RegE, Begründung zu Nummer 14).

Die Regelung ist jedoch so weit formuliert, dass sie Zahlungseingänge auf irgendeinem Bankkonto (und damit korrespondierende einzelne Zahlungsausgänge vom Konto eines Kunden) erfasst.

#### Beispiel

Ein Versicherungsunternehmen bewertet, u. a. anhand der ihm selbst vorliegenden Daten über Beitragszahlungen, die Bereitschaft eines Kunden, seine Versicherungsverträge zu erfüllen. Dieser Wahrscheinlichkeitswert soll an die Stelle des Scorewertes einer Auskunft treten oder diesen ergänzen. Er ist in aller Regel in der jeweiligen Konstellation treffsicherer als ein allgemeiner Wert einer Auskunft.

Nicht zulässig wären im Beispielfall nach dem Wortlaut des § 37a Abs. 2 Nr. 1 Buchst. c) BDSG-RegE die Einbeziehung von Zahlungseingängen auf dem Konto des Versicherungsunternehmens selbst, denen einzelne Zahlungsausgänge von dem Konto des Kunden entsprechen. Der Wortlaut der Norm geht weit über den Regelungszweck des § 37a Abs. 2 Nr. 1 Buchst. c) BDSG-RegE hinaus. Denn hier kann das Versicherungsunternehmen keine umfassenden Erkenntnisse über persönliche Aspekte der Lebensführung des Kunden gewinnen, weil es nur punktuell die Zahlungsvorgänge betrachtet, die es selbst angehen.

Um sich nicht auf eine im Ergebnis unsichere teleologische Reduktion des § 37a Abs. 2 Nr. 1 Buchst. c) BDSG-RegE verlassen zu müssen, sollte der Wortlaut der Norm präziser gefasst werden.

#### Vorschlag der deutschen Versicherungswirtschaft

§ 37a Abs. 2 Nr. 1 Buchst. c) BDSG-RegE sollte wie folgt präzisiert werden:

„Informationen über eine Vielzahl verschiedener Zahlungseingänge und -ausgänge auf und von Bankkonten der vom Scoring betroffenen Person, durch deren Zusammenspiel neue Erkenntnisse über persönliche Aspekte der Lebensführung der vom Scoring betroffenen Person gewonnen werden

können,“

## **1.2 Keine anderen Zwecke (§ 37a Abs. 2 Nr. 3 Buchst. b) BDSG-RegE)**

Nach § 37a Abs. 2 Nr. 3 Buchst. b) BDSG-RegE dürfen die genutzten personenbezogenen Daten für keine anderen Zwecke verarbeitet werden.

Diese Anforderung ist für ein Versicherungsunternehmen, das mit eigenen Daten Wahrscheinlichkeitswerte errechnet, nicht einzuhalten. Wenn ein Versicherungsunternehmen einen eigenen Wahrscheinlichkeitswert errechnet, der den von einer Auskunftsei errechneten Wert ersetzen oder ergänzen soll, geschieht dies immer mit Daten, die bereits vorher zu einem anderen Zweck verarbeitet wurden und auch nachfolgend noch zu anderen Zwecken dienen können.

### **Beispiel**

Das Unternehmen bewertet anhand der ihm vorliegenden Zahlungseingänge seines Kunden zu verschiedenen Verträgen dessen Bereitschaft, künftig Versicherungsverträge zu erfüllen. Die Information, dass der Kunde die Versicherungsprämie für einen bestimmten Vertrag nicht gezahlt hat, dient auch dem Zweck, den Kunden zu mahnen bzw. weitere Schritte zum Inkasso einzuleiten.

Da sich eine Zweckbindung ohnehin aus Art. 6 Abs. 4 DSGVO ergibt, ist die Regelung nicht nötig. Sie sollte gestrichen oder zumindest auf Auskunftseien beschränkt werden.

### **Vorschlag der deutschen Versicherungswirtschaft**

§ 37a Abs. 2 Nr. 3 Buchst. b) BDSG-RegE sollte gestrichen oder zumindest wie folgt präzisiert werden:

„in den Fällen des § 37a Abs. 1 Nr. 2 BDSG für keine anderen Zwecke verarbeitet werden.“

## **1.3 Keine unerlaubte Konkretisierung des Art. 6 DSGVO durch § 37a Abs. 2 BDSG-RegE**

Es ist nicht auszuschließen, dass der Gesetzestext des § 37a Abs. 2 BDSG-RegE dahingehend interpretiert wird, dass die in § 37a Abs. 1 Nr. 1 und 2 genannten Wahrscheinlichkeitswerte immer die Anforderungen des § 37a Abs. 2 BDSG-RegE erfüllen müssen, unabhängig davon, ob von der Ausnahme nach § 37a Abs. 1 BDSG-RegE oder einer anderen Ausnahme des Art. 22 Abs. 2 DSGVO Gebrauch

gemacht wird. Eine solche Regelung wäre dann aber – wie der EuGH es für § 31 BDSG erwägt – nur eine Konkretisierung der allgemeinen Erlaubnisnorm des Art. 6 DSGVO. Sie wäre somit nach der Rechtsprechung des EuGH (Urteil vom 07.12.2023, a. a. O., Rn. 68 ff.) nicht wirksam.

Die Absicht des Gesetzgebers, in § 37a Abs. 2 BDSG-RegE lediglich die auf Art. 22 Abs. 2 lit. b) DSGVO gestützte und in § 37a Abs. 1 BDSG-RegE formulierte Ausnahme vom Verbot des Art. 22 Abs. 1 DSGVO zu konkretisieren, sollte nicht nur in der Gesetzesbegründung sondern auch im Gesetzestext deutlich werden.

#### **1.4 Schutz von Geschäftsgeheimnissen (§ 37a Abs. 5 BDGS-RegE)**

§ 37a Abs. 5 BDGS-RegE schließt die Anwendung des neu geschaffenen § 34 Abs. 1 Satz 2 BDSG-RegE im Anwendungsbereich des § 37a BDSG-RegE vollständig aus. Damit kann der Ersteller eines Wahrscheinlichkeitswertes einem Auskunftersuchen nach § 37a Abs. 4 BDSG-RegE ein Geschäftsgeheimnis unter keinen Umständen entgegenhalten.

Es ist wichtig, dass die betroffene Person nachvollziehen kann, welche Kriterien bei der Ermittlung des Wahrscheinlichkeitswertes eine Rolle gespielt haben und letztlich für die Entscheidung maßgeblich waren. Andererseits müssen Unternehmen davor geschützt werden, dass § 37a Abs. 4 BDSG-RegE extensiv ausgelegt wird und Berechnungsformeln, die im Wettbewerb eine wichtige Rolle spielen, bekannt gemacht werden müssen. Diese gegenläufigen Interessen berücksichtigt § 34 Abs. 1 Satz 2 BDSG-RegE, indem er die Verweigerung der Auskunft nur zulässt, wenn das Interesse an der Geheimhaltung das Interesse der betroffenen Person an der Information überwiegt. Er sollte daher anwendbar bleiben.

Zudem ist der Wortlaut des § 37a Abs. 5 RegE sehr weit formuliert und wird erst durch die Begründung eingeschränkt. Dies kann zu Missverständnissen führen.

#### **Vorschlag der deutschen Versicherungswirtschaft:**

§ 37a Abs. 5 BDSG-RegE sollte gestrichen werden.

## **2. Vollautomatisierte Einzelentscheidungen zur Risiko- und Leistungsprüfung in der Versicherungswirtschaft (§ 37 BDSG)**

Sinnvoll ist die Klarstellung in § 37a Abs. 1 BDSG-RegE, dass Artikel 22 Abs. 2 Buchst. a) und c) DSGVO von der neuen Regelung unberührt bleiben. Denn der europäische Gesetzgeber hat vollautomatisierte Einzelentscheidungen, die zum Abschluss eines Vertrages erforderlich sind bzw. die mit wirksamer Einwilligung

erfolgen, erlaubt. Diese Erlaubnis kann der deutsche Gesetzgeber nicht einschränken, sondern über die Öffnungsklausel des Artikel 22 Abs. 2 Buchst. b) lediglich weitere Erlaubnisgrundlagen schaffen.

Aktuell wird die Digitalisierung von Risiko- und Leistungsprüfungen in der Versicherungswirtschaft allerdings dadurch behindert, dass Artikel 22 Abs. 2 Buchst. a) und c) DSGVO von den Datenschutzbehörden sehr restriktiv ausgelegt werden. Sie enthalten zudem keine Lösung für die Prüfung und Regulierung von Ansprüchen, die nicht Vertragspartner, sondern dritte Personen (zum Beispiel Geschädigte in der Haftpflichtversicherung) geltend machen.

Das Versicherungsgeschäft ist ein Massengeschäft. Unsere Mitgliedsunternehmen verwalten mehr als 465 Mio. Versicherungsverträge. Sie regulieren Schäden und erbringen Leistungen in Höhe von jährlich mehr als 180 Mrd. Euro. Könnten die vollautomatisierte Risikoprüfung beim Vertragsschluss sowie die Leistungsprüfung und -abwicklung im Schadenfall vollautomatisiert erfolgen, würden Kunden und Geschädigte unkomplizierter und erheblich schneller als bei manueller Bearbeitung Versicherungsschutz bzw. die ihnen im Versicherungsfall zustehenden Leistungen erhalten.

Um der Digitalisierung in der Versicherungswirtschaft angemessen Rechnung zu tragen, wäre es hilfreich, § 37 BDSG so anzupassen, dass vollautomatisierte Entscheidungen zum Abschluss und zur Durchführung eines Versicherungsvertrages, einschließlich der Regulierung von Ansprüchen Dritter in der Haftpflichtversicherung grundsätzlich zulässig sind, wenn Transparenz über die Entscheidung und ein Recht auf menschliche Überprüfung bestehen.

### **Vorschlag der deutschen Versicherungswirtschaft**

§ 37 BDSG sollte auch den Abschluss und die Durchführung von Versicherungsverträgen erfassen und nicht auf Entscheidung über die Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beschränkt sein.

Einzelheiten, Beispiele und ein konkreter Formulierungsvorschlag sind Ziffer 4.2.2. unserer [Stellungnahme zu dem Referentenentwurf](#) zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes zu entnehmen.

## **3. Zuständigkeit der Datenschutzaufsichtsbehörden**

§ 40a und § 27 Abs. 5 BGG-RegE, die es ermöglichen, die Zuständigkeit einer einzigen Landesdatenschutzaufsichtsbehörde für gemeinsame Vorhaben mehrerer Verantwortlicher zu begründen, sind ein guter Schritt in die richtige Richtung. Sie verhindern divergierende Entscheidungen unterschiedlicher Behörden in

gleichgelagerten Sachverhalten und dienen damit der im Koalitionsvertrag vorgesehenen besseren Durchsetzung und Kohärenz des Datenschutzes.

Allerdings sollte § 40a BDSG-RegE **über die gemeinsame Verantwortlichkeit hinaus für jede Datenverarbeitung in einer Unternehmensgruppe** gelten. Nicht jede Datenverarbeitung innerhalb eines Konzerns ist eine gemeinsame Verantwortlichkeit im Sinne von Art. 26 DSGVO. Es kommt nicht selten vor, dass ein Prozess abstrakt konzernweit gestaltet wird, die Verarbeitung personenbezogener Daten aber dann in alleiniger Verantwortung der jeweiligen Konzerngesellschaften ausgeführt wird. Auch in derartigen Fällen ist es problematisch, wenn durch den Sitz der jeweiligen Konzernunternehmen unterschiedliche Aufsichtsbehörden zuständig sind und ggf. unterschiedliche Ansichten zur Zulässigkeit der Verarbeitung vertreten. In Erwägungsgrund 48 erkennt die DSGVO ausdrücklich das berechnete Interesse an Datenflüssen innerhalb von Unternehmensgruppen an. Daher sollte § 40a BDSG neben Fällen der gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO generell auf die Datenverarbeitung innerhalb einer Unternehmensgruppe erweitert werden.

Außerdem erscheint es **zu starr**, zwingend die Zuständigkeit der Aufsichtsbehörde anzunehmen, in deren Zuständigkeitsbereich das Unternehmen fällt, das in dem der Antragstellung vorangegangenen Geschäftsjahr den größten weltweiten **Jahresumsatz** erzielt hat. So kann innerhalb eines Versicherungskonzerns ein operativ tätiges Tochterunternehmen den höchsten Umsatz haben, während die maßgebenden Entscheidungen für die Datenverarbeitung in der Konzernholding oder einer Servicegesellschaft getroffen werden. Art. 26 DSGVO lässt den gemeinsam Verantwortlichen einen weitgehenden Spielraum bei der Ausgestaltung ihrer Rechte und Pflichten, solange darüber Transparenz besteht. So können sie z. B. nach Art. 26 Abs. 1 Satz 2 DSGVO in transparenter Form festlegen, wer von ihnen welche Verpflichtung nach der DSGVO erfüllt. Daher spricht auch nichts dagegen, dass die Unternehmen festlegen, wer das „führende“ Unternehmen ist. Die Datenschutzbehörde, in deren Zuständigkeitsbereich dieses Unternehmen fällt, wäre dann zuständig.

### **Vorschlag der deutschen Versicherungswirtschaft**

§ 40a BDSG-RefE sollte über die gemeinsame Verantwortlichkeit hinaus auf die Datenverarbeitung in einer Unternehmensgruppe erweitert werden.

Die Zuständigkeit der Datenschutzbehörden sollte daran anknüpfen, welches Unternehmen die Verantwortlichen für den Verarbeitungsprozess vertraglich als führend festgelegt haben.

#### 4. Weitere Vorschläge

In unserer [Stellungnahme zu dem Referentenentwurf](#) eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes haben wir weitere Vorschläge unterbreitet, die mehr Rechtssicherheit schaffen und die Digitalisierung erleichtern würden. Dazu gehören nationale gesetzliche Erlaubnisgrundlagen für die Verarbeitung von Gesundheitsdaten in der Versicherungswirtschaft (Ziffer 4.3.) und für die Verarbeitung von Daten über Straftaten und strafrechtliche Verurteilungen im Sinne von Art. 10 DSGVO (Ziffer 4.4.). Ferner fordern wir klare Rechtsnormen für die Anonymisierung und Pseudonymisierung sowie für die Entwicklung und für Tests von IT-Anwendungen, Produkten und Systemen (Ziffer 4.5.). Schließlich regen wir Klarstellungen in den Regelungen zu den Betroffenenrechten an (Ziffer 4.6.).

Wegen Einzelheiten dieser Forderungen verweisen wir auf unsere Stellungnahme zu dem Referentenentwurf.

Berlin, den 28.02.2024