GDV Gesamtverband der Versicherer

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)448

STELLUNGNAHME

Stellungnahme

des Gesamtverbandes der
Deutschen Versicherungswirtschaft
Lobbyregister-Nr. R000774

zum Regierungsentwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes

Inhalt

GDV

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

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

Ansprechpartner
Datenschutz/Grundsatzfragen

E-Mail
data-protection@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 Auskunfteien 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 Auskunfteien 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 Auskunftei treten oder diesen ergänzen. Er ist in aller Regel in der jeweiligen Konstellation treffsicherer als ein allgemeiner Wert einer Auskunftei.

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 Auskunftei 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 Auskunfteien 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 Auskunftsersuchen 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 BGSG-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 konzerneinheitlich 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 berechtigte 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 Rechtnormen 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

GDV Gesamtverband der Versicherer

STELLUNGNAHME

Stellungnahme

des Gesamtverbandes der
Deutschen Versicherungswirtschaft
Lobbyregister-Nr. R000774

zum Referentenentwurf
eines Ersten Gesetzes zur Änderung des
Bundesdatenschutzgesetzes vom 9. August 2023

GDV

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

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

Ansprechpartner
Datenschutz/Grundsatzfragen

E-Mail
datenschutz@gdv.de

1. Inhalt

2. Zusammenfassung

Die Novellierung des BDSG sollte unbedingt genutzt werden, um der Datenstrategie der Bundesregierung in der Praxis zur Geltung zu verhelfen. Erste ausbaufähige Ansätze des Referentenentwurfs (BDSG-RefE) sind die Regelungen zur Zuständigkeit einer Datenschutzaufsichtsbehörde bei gemeinsam Verantwortlichen (§ 40a und § 27 Abs. 5 BDSG-RefE – dazu Punkt 4.1. dieser Stellungnahme) sowie die Einschränkung des Auskunftsrechts zum Schutz von Geschäftsgeheimnissen (§ 34 BDSG-RefE – Dazu Punkt 4.6.1).

Aus Sicht der Versicherungswirtschaft sind weitere Regelungen nötig, um Datennutzung und Digitalisierung voranzubringen:

§ 37 BDSG sollte **vollautomatisierte Entscheidungen** der Versicherer bei Vertragsabschlüssen und bei der Prüfung von Leistungsansprüchen erlauben, um im Massengeschäft Kunden und Geschädigte schnell und unkompliziert bedienen zu können. § 37 Abs. 1 Nr. 1 BDSG sollte nicht gestrichen werden (dazu Punkt 4.2).

- In das BDSG sollte nach dem Vorbild anderer EU-Staaten eine eindeutige gesetzliche Erlaubnisgrundlage für die Verarbeitung von Gesundheitsdaten zum Abschluss und zur Durchführung von Versicherungsverträgen aufgenommen werden (dazu Punkt 4.3.).

- In das BDSG sollte eine eindeutige Rechtsgrundlage i. S. v. Art. 10 DSGVO für die **Verarbeitung von Daten über Straftaten** und strafrechtliche Verurteilungen in der Versicherungswirtschaft eingefügt werden (dazu Punkt 4.4.).

- Es sollten – insbesondere für besondere Kategorien personenbezogener Daten – eindeutige Rechtsgrundlagen für die **Anonymisierung und Pseudonymisierung von Daten** sowie für die **Nutzung pseudonymisierter Daten zur Entwicklung und zum Test neuer Anwendungen und Systeme** geschaffen werden (dazu Punkt 4.5).

- Schließlich sollten **Unstimmigkeiten in den Ausnahmen zu den Betroffenenrechten beseitigt** werden (dazu Punkt 4.6.2. und 4.6.3)

3. Einleitung

In dem RefE-BDSG sollen die datenschutzrechtlich relevanten Vereinbarungen im Koalitionsvertrag und die Ergebnisse der Evaluierung des Bundesdatenschutzgesetzes im Jahr 2021 umgesetzt werden. Insofern sind die Regelungen in § 40a und § 27 Abs. 5 RefE und § 34 RefE ein Schritt in die richtige Richtung**.**

Die BDSG-Novellierung sollte jedoch darüber hinaus genutzt werden, um den richtigen Ansätzen in der Datenstrategie der Bundesregierung in der Praxis zur Geltung zu verhelfen. In dem dazu kürzlich veröffentlichten Papier „Fortschritt durch Datennutzung“ führt die Bundesregierung auf den Seiten 20 und 21 aus, dass sie den Datenschutz „einfacher, kohärenter und praktikabler“ machen will. Die Ziele, einen „ermöglichenden Datenschutz“ zu schaffen, indem „Spielräume und Öffnungsklauseln der DSGVO“ durch neue „gesetzliche Erlaubnistatbestände, Regelbeispiele und Klarstellungen …“ genutzt werden, unterstützen wir uneingeschränkt.

Wir regen dringend an, diese Ziele schon mit der BDSG-Novellierung in konkreten Regelungen umzusetzen, um den Anschluss an die Digitalisierung nicht zu verpassen.

4. Stellungnahme zu einzelnen Bestimmungen

Zu dem Referentenentwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes vom 9. August 2023 **(RefE-BDSG)** nehmen wir nachfolgend im Einzelnen Stellung.

4.1. Zuständigkeit der Datenschutzaufsichtsbehörden

Die Regelungen in § 40a und § 27 Abs. 5 RefE, die die Zuständigkeit einer einzigen Landesdatenschutzaufsichtsbehörde für gemeinsame Vorhaben mehrerer Verantwortlicher 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.

4.1.1. Anknüpfungspunkt und Maßstab des § 40a BDSG

Es ist zu begrüßen, dass § 40a BDSG für den Fall der gemeinsamen Verantwortlichkeit im Sinne von Art. 26 DSGVO die Möglichkeit schafft, dass nur eine Datenschutzbehörde zuständig ist.

Allerdings sollte diese Möglichkeit **über die gemeinsame Verantwortlichkeit hinaus für jede Datenverarbeitung in einer Unternehmensgruppe** geschaffen werden. 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 konzerneinheitlich gestaltet wird, aber dann in alleiniger Verantwortung der jeweiligen Konzerngesellschaften ausgeführt wird, z. B. weil unterschiedliche IT-Systeme zu Grunde liegen. 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 berechtigte 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.

Schließlich 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 **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.

Die deutsche Versicherungswirtschaft schlägt daher vor

- **§ 40a BDSG-RefE über die gemeinsame Verantwortlichkeit hinaus auf die Datenverarbeitung in einer Unternehmensgruppe zu erweitern und**
- **die Zuständigkeit der Datenschutzbehörden daran anzuknüpfen, welches „führende“ Unternehmen die Verantwortlichen für den Verarbeitungsprozess vertraglich festgelegt haben.**

4.1.2. Zu enge Regelung in § 27 Abs. 5 BDSG

Es ist nicht nachvollziehbar, wieso sich die Erleichterung für gemeinsam Verantwortliche, die nicht oder nicht ausschließlich Unternehmen sind, auf den eng

begrenzten Fall des § 27 BDSG beziehen soll. Damit sind nur Vorhaben erfasst, bei denen besondere Kategorien personenbezogener Daten i. S. v. Art. 9 Abs. 1 DSGVO für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke verarbeitet werden. Es sind aber zahlreiche weitere Zwecke denkbar, in denen eine enge Zusammenarbeit von öffentlichen und privaten Stellen die Zuständigkeit einer einzigen Landesdatenschutzbehörde sinnvoll erscheinen lässt. Zu denken ist etwa an Maßnahmen zur Vermeidung oder Behebung öffentlicher Notstände oder an Forschungsvorhaben, die nicht die Verarbeitung besonderer Kategorien personenbezogener Daten erfordern.

Die deutsche Versicherungswirtschaft schlägt daher vor

die Regelung allgemeiner zu fassen und in § 40a BDSG zu integrieren.

4.2. Vollautomatisierte Einzelentscheidungen in der Versicherungswirtschaft (§ 37 BDSG)

§ 37 BDSG hat im Massengeschäft der Versicherungswirtschaft eine erhebliche Bedeutung. Um Rechtssicherheit zu erhalten und den Anforderungen der Digitalisierung gerecht zu werden, sollte nicht § 37 Abs. 1 Nr. 1 BDSG gestrichen, sondern die Norm insgesamt überarbeitet werden.

4.2.1. Keine Streichung des § 37 Abs. 1 Nr. 1 BDSG

Nach den Vorschlägen zur Änderung des § 37 BDSG (Artikel 1, Ziffer 11 RefE-BDSG) soll § 37 Abs. 1 Nr. 1 BDSG gestrichen werden.

§ 37 Abs. 1 Nr. 1 BDSG erlaubt bisher ausdrücklich vollautomatisierte Entscheidungen von Versicherungsunternehmen im Einzelfall, mit denen dem Antrag von Kunden bzw. Geschädigten auf eine Versicherungsleistung entsprochen wird. Die Streichung wird damit begründet, dass eine Entscheidung, die einem Begehren der betroffenen Person vollumfänglich stattgibt, schon nicht unter das Verbot der automatisierten Entscheidung nach Artikel 22 Abs.1 DSGVO falle. Die Norm solle nur vor solchen Entscheidungen schützen, die mit einer beeinträchtigenden Wirkung für die betroffene Person verbunden sind (RefE-BDSG, Begründung zu Nr. 11).

Wir halten diese Rechtsauffassung des Ministeriums zwar für sehr gut vertretbar. Sie wird auch in der Literatur geteilt (z. B. Buchner in Kühling/Buchner, Art. 22 Rn. 25; Herbst in Auernhammer, Art. 22 Rn. 14). Eine starke Gegenmeinung geht jedoch immer noch davon aus, dass Art. 22 Abs. 1 DSGVO auch stattgebende Entscheidungen grundsätzlich verbietet (z. B. Helfrich in Sydow/Marsch, Art. 22 Rn. 48; Martini in Paal/Pauly, Art. 22 Rn. 26; Weichert in Däubler/Wedde/

Weichert/Sommer, Art. 22 Rn. 27), sodass hier keine Rechtssicherheit besteht.

Den vom Europäischen Datenschutzausschuss (EDSA) übernommenen Leitlinien WP 251 rev. 01 der Artikel-29-Gruppe (S. 23) und auch den Schlussanträgen des Generalanwalts in der vor dem EuGH anhängigen Rechtssache C 634/21 (Rn. 34) ist lediglich zu entnehmen, dass Art. 22 nur „schwerwiegende Auswirkungen“ erfassen soll. Dies lässt sich zwar dahingehend interpretieren, dass stattgebende Entscheidungen nicht von der Norm erfasst werden, jedoch ist auch dies nicht eindeutig. Gemeint sein könnte auch, dass jede Entscheidung erfasst ist, die potenziell schwerwiegende Beeinträchtigungen zur Folge haben kann. Auch die deutschen Datenschutzbehörden haben bisher nicht bestätigt, dass Art. 22 Abs. 1 DSGVO stattgebende Entscheidungen nicht erfasst.

Die Rechtslage bleibt daher unsicher, solange keine Entscheidung des EuGH vorliegt.

Um die Rechtssicherheit für die Versicherungswirtschaft bis zu einer Entscheidung des EuGH zu erhalten, schlagen wir daher vor,

§ 37 Abs. 1 Nr. 1 BDSG nicht zu streichen.

4.2.2. Anpassung der Ausnahmen in § 37 BDSG für automatisierte Einzelfallentscheidungen in der Versicherungswirtschaft

Um der Digitalisierung in der Versicherungswirtschaft angemessen Rechnung zu tragen, halten wir es darüber hinaus für geboten, § 37 BDSG so anzupassen, dass in diesem Bereich vollautomatisierte Entscheidungen grundsätzlich zulässig sind.

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. Durch die vollautomatisierte Leistungsprüfung und -abwicklung erhalten Kunden und Geschädigte unkomplizierter und erheblich schneller als bei manueller Bearbeitung die ihnen zustehenden Leistungen. Im Zuge zunehmender Digitalisierung müssen Versicherer auch in der Lage sein, vollautomatisiert über Anträge auf Versicherungsschutz zu entscheiden. Nur so kann den Wünschen der Kunden, die eine schnelle Bearbeitung ihrer Anliegen erwarten, Rechnung getragen werden.

Beispiele:

- Ein Kunde möchte eine Unfallversicherung noch vor einem Sporturlaub am Wochenende elektronisch abschließen. Der Versicherer bietet hierfür einen Online-Abschluss mit einer Gesundheitsfrage an.
- Ein Unfallversicherer zahlt bei einem Krankenhausaufenthalt Krankentagegeld aus. Der Kunde beantragt Tagegeld für 11 Tage, legt aber eine Bescheinigung vor, aus der hervorgeht, dass er nur 10 Tage lang im Krankenhaus war. Die Bescheinigung wird automatisiert ausgelesen, der Bescheid wird automatisiert erstellt und verschickt und der Kunde erhält sofort Krankentagegeld für 10 Tage. Wegen des verbleibenden Tages kann er sich mit seinem Versicherer in Verbindung setzen, sofern er weiterhin der Ansicht ist, hierfür Ersatz beanspruchen zu können.

In dem zuerst genannten Beispiel wären nach § 37 BDSG in der aktuellen Fassung vollautomatisierte Entscheidungen nicht ausdrücklich erlaubt, weil § 37 BDSG das Antragsverfahren nicht abdeckt. Im zweiten Beispiel wäre keine vollautomatisierte Entscheidung möglich, weil dem Begehren nicht vollumfänglich stattgegeben wird und der in § 37 Abs. 1 Nr. 2 genannte Sonderfall (Krankenversicherung) nicht vorliegt.

Die in Art. 22 Abs. 2 DSGVO enthaltenen Ausnahmen helfen zurzeit in der Praxis nicht weiter, denn sie werden von den Datenschutzbehörden sehr eng ausgelegt. Die Behörden betrachten vollautomatisierte Entscheidungen als nicht „erforderlich“ für den Abschluss oder die Erfüllung des Versicherungsvertrages im Sinne von Art. 22 Abs. 2 lit. a) DSGVO, da der Vertrag auch manuell abgeschlossen und durchgeführt werden könne. Ist die betroffene Person nicht selbst der Vertragspartner des Versicherers (z. B. ein von der versicherten Person geschädigter Dritter in der Kfz-Haftpflichtversicherung), greift die Ausnahme nach Art. 22 Abs. 2 Buchst. a) DSGVO gar nicht. Daher ist für diese in der Praxis häufige Konstellation unbedingt eine Regelung nötig. Für diesen Fall erkennt auch bereits der **Evaluierungsbericht** des BMI zum BDSG auch dem Jahr 2021 den Regelungsbedarf (S. 52). Auch Einwilligungen gemäß Art. 22 Abs. 2 lit. c) DSGVO ermöglichen keine vollautomatisierte Entscheidung, denn die deutschen Datenschutzbehörden sehen diese nur dann als freiwillig an, wenn das Unternehmen von Anfang an eine menschliche Prüfung als frei wählbare Alternative anbietet. Die in Art. 22 Abs. 3 DSGVO ohnehin vorgesehene menschliche Prüfung auf Wunsch des Kunden nach der Entscheidung (also sozusagen auf zweiter Stufe) reicht den Behörden nicht aus.

Vorschlag der deutschen Versicherungswirtschaft:

Dem dargestellten Bedarf und dem von Artikel 1 Ziffer 11 des Referentenentwurfs verfolgten Zeil könnte rechtssicher mit einer Änderung des § 37 BDSG Rechnung getragen werden. Die dazu erforderlichen Öffnungen enthält die DSGVO in Art. 22 Abs. 2 lit. b) und Art. 22 Abs. 4 i. V. m. Art. 9 Abs. 2 lit. g) DSGVO.

Wir schlagen daher vor, **§ 37 BDSG Abs. 1 wie folgt zu ändern**:

(1) Das Recht gemäß Artikel 22 Absatz 1 der Verordnung (EU) 2016/679, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, besteht über die in Artikel 22 Absatz 2 Buchstabe a und c der Verordnung (EU) 2016/679 genannten Ausnahmen hinaus nicht, wenn die Entscheidung im Rahmen **des Abschlusses eines Versicherungsvertrages oder** der Leistungserbringung nach einem Versicherungsvertrag ergeht und

1. dem Begehren der betroffenen Person stattgegeben wurde oder

2. ~~**die Entscheidung auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruht und**~~ der Verantwortliche für den Fall, dass dem Antrag nicht vollumfänglich stattgegeben wird, angemessene Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person trifft, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunktes und auf Anfechtung der Entscheidung zählt; der Verantwortliche informiert die betroffene Person über diese Rechte spätestens im Zeitpunkt der Mitteilung, aus der sich ergibt, dass dem Antrag der betroffenen Person nicht vollumfänglich stattgegeben wird.

4.3. Eindeutige gesetzliche Erlaubnisnorm für die Verarbeitung von Gesundheitsdaten zu Versicherungszwecken (§ 22 BDSG)

In § 22 BDSG sollte eine eindeutige gesetzliche Erlaubnisgrundlage für die Verarbeitung von Gesundheitsdaten zum Abschluss und zur Durchführung von Versicherungsverträgen (einschließlich der Rückversicherung) aufgenommen werden. Zumindest sollte die Anwendbarkeit des Art. 9 Abs. 2 lit. f) DSGVO, der die Verarbeitung von Gesundheitsdaten zur Geltendmachung, Ausübung und Verteidigung rechtlicher Ansprüche erlaubt, auf die Durchführung von Versicherungsverträgen in der Gesetzesbegründung klargestellt werden.

In der Lebens-, Kranken- und Unfallversicherung (einschließlich der Rückversicherung) können Verträge nur abgeschlossen und durchgeführt werden, wenn Gesundheitsdaten verarbeitet werden. Gesundheitsdaten müssen aber auch in der Haftpflicht- und Rechtsschutzversicherung verarbeitet werden, wenn Ansprüche wegen Gesundheitsschäden geltend gemacht werden.

Nach Auffassung der deutschen Versicherungswirtschaft ist die zur Durchführung eines Versicherungsvertrages erforderliche Verarbeitung von Gesundheitsdaten nach Art. 9 Abs. 2 lit. f) DSGVO erlaubt. Denn hier geht es um die Durchsetzung bzw. Abwehr von Ansprüchen. Die Rechtslage ist allerdings unsicher. Von den deutschen Datenschutzbehörden wird dies überwiegend abgelehnt.

Andere EU-Länder verfügen über spezielle nationale Erlaubnisnormen unterschiedlichen Umfangs zur Verarbeitung von Gesundheitsdaten zum Abschluss und/oder zur Durchführung eines Versicherungsvertrages. Ein Beispiel ist § 11a des österreichischen Versicherungsvertragsgesetzes. Andere Länder, z. B. Bulgarien, Niederlande, Polen, Slowakei und Spanien haben entsprechende spezielle Regelungen. Die Regelungen basieren z. T. auf Art. 9 Abs. 2 b), g) bzw. h) DSGVO oder sie werden auf Art. 9 Abs. 4 DSGVO gestützt. Teils werden sie auch als Konkretisierungen des Art. 9 Abs. 2 lit. f) DSGVO verstanden. Die Datenschutzbehörden einiger EU-Länder, z. B. Dänemark und Tschechien, wenden Art. 9 Abs. 2 lit. f) DSGVO direkt an.

Greift keine gesetzliche Erlaubnis, muss die Verarbeitung der Gesundheitsdaten auf eine Einwilligung nach Art. 9 Abs. 2 lit. a), Art. 7 DSGVO gestützt werden. **Die Verhandlung einer Muster-Einwilligung zwischen der deutschen Versicherungswirtschaft und der Datenschutzkonferenz dauert inzwischen schon mehr als vier Jahre an**. Inzwischen greifen einzelne Datenschutzbehörden die Einwilligung sogar als unfreiwillig an[1], sodass nicht einmal mehr auf diese Weise Rechtssicherheit erzielt werden kann.

Die unklare Rechtslage führt zu kritischen Nachfragen von Geschädigten und ihren Rechtsanwälten, die die Einholung einer Einwilligung als Versuch der Versicherungswirtschaft ansehen, die Schadenregulierung zu verzögern. Es kommt schließlich zu Schwierigkeiten im grenzüberschreitenden Datenverkehr mit Ländern, in denen Versicherer keine Einwilligung einholen müssen. Deren Rückversicherer mit Sitz in Deutschland erhalten keine Einwilligung über den ausländischen Erstversicherer. Sie haben aber auch keinen direkten Kontakt zu dem Kunden in dem anderen Land, um dessen Einwilligung einzuholen.

Eine eindeutige gesetzliche Erlaubnisgrundlage für die Datenverarbeitung zum

[1] 5. Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen über das Ergebnis der Tätigkeit im Jahr 2022, Ziffer 16.8, S. 75.

Abschluss und zur Durchführung von Versicherungsverträgen würde für deutsche Erst- und Rückversicherer die dringend benötigte Rechtsklarheit schaffen. Sie würde den Datentransfer zur Abwicklung des Versicherungsgeschäfts auf europäischer Ebene erleichtern und diese Standortnachteile deutscher Erst- und Rückversicherer aufheben. Zudem würde die Regelung verhindern, dass bei einem Widerruf der Einwilligung Vertragsrecht und Datenschutzrecht auseinanderlaufen. Die Erbringung der vertraglich geschuldeten Leistungen würde nicht an einer ggf. fehlenden Einwilligung scheitern.

Vorschlag der deutschen Versicherungswirtschaft:

Wir schlagen vor, in § 22 Abs. 1 Nr. 1 BDSG eine **gesetzliche Erlaubnisgrundlage für die Datenverarbeitung zum Abschluss und zur Durchführung von Versicherungsverträgen einschließlich der Rückversicherung und der Regulierung von Drittansprüchen in der Haftpflichtversicherung** aufzunehmen. Vorbild könnte § 11a Abs. 1 des österreichischen Versicherungsvertragsgesetzes sein.

Hilfsweise würde aber auch schon eine **Klarstellung in der Begründung zu § 22 BDSG**, dass diese Verarbeitung von Gesundheitsdaten nach Art. 9 Abs. 2 lit. f) DSGVO als Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erlaubt ist, für Rechtssicherheit sorgen.

Ferner verweisen wir auf die Forderungen in der Stellungnahme des PKV-Verbandes, die wir ebenfalls unterstützen.

4.4. Rechtssicherheit für die Verarbeitung von Daten über Straftaten und strafrechtliche Verurteilungen (Art. 10 DSGVO)

Die Versicherungswirtschaft ist darauf angewiesen, Daten über Straftaten und strafrechtliche Verurteilungen zu verarbeiten. Das gilt insbesondere für die Erfüllung der Anforderungen an die **Überprüfung der Zuverlässigkeit von Personen in Leitungs- und Schlüsselfunktionen** sowie von Versicherungsvermittlern. Daten über Straftaten können darüber hinaus in **vielfältigen Konstellationen beim Abschluss und der Durchführung von Versicherungsverträgen** anfallen.

Beispiele:

- Versicherungsunternehmen sind zur Überprüfung der Zuverlässigkeit von Personen in Leitungs- und Schlüsselfunktionen nach Art. 273 Nr. 4 VO(EU) 2015/35 sowie von Versicherungsvermittlern nach Art. 10 Abs. 3 der Richtlinie (EU) 2016/97 verpflichtet. Dazu müssen sie Führungszeugnisse nach dem

Bundeszentralregistergesetz oder vergleichbare Unterlagen anfordern, aus denen sich ggf. strafrechtliche Verurteilungen ergeben. Wenn es später zu einer Straftat der Personen gekommen ist, müssen sie nachweisen können, dass sie eine entsprechende Prüfung vorgenommen haben.

- Bei der Strafrechtsschutzversicherung sind Straftaten, strafrechtliche Ermittlungen, Verfahren und Verurteilungen Leistungsauslöser für den Versicherungsschutz, aber auch für die Entscheidung über den Abschluss eines Versicherungsvertrages relevant.
- Hat ein Arbeitnehmer eine Rechtsschutzversicherung abgeschlossen und wird sein Arbeitsverhältnis wegen einer (vermeintlich oder tatsächlich begangenen) Straftat oder Verurteilung gekündigt, muss der Versicherer den Fall bearbeiten können.
- Geschädigte begründen Ansprüche damit, dass der Schädiger eine Straftat begangen hat, z. B. ein Verkehrsdelikt in der Kraftfahrt-Haftpflichtversicherung.
- In der Gebäudeversicherung wird geprüft, ob Brandstiftung vorliegt.

Außerdem müssen Unternehmen in der Lage sein, einen gegen sie gerichteten Betrug abzuwehren und erfahren dabei ggf. auch von einer strafrechtlichen Verurteilung. Die DSGVO bejaht ausdrücklich ein berechtigtes Interesse des für die Datenverarbeitung Verantwortlichen zur Betrugsabwehr (ErwGr. 47, Satz 6 DSGVO). Schließlich muss eine Verarbeitung von Daten über Straftaten und strafrechtliche Verurteilungen auch möglich sein, um durch eine strafbare Handlung entstandene zivilrechtliche Ansprüche durchsetzen zu können.

In allen genannten Fällen ist die Datenverarbeitung nach Art. 6 DSGVO zulässig.

Gemäß Art. 10 DSGVO dürfen Daten über Straftaten und strafrechtliche Verurteilungen auf Grundlage von Art. 6 Abs. 1 DSGVO aber nur verarbeitet werden

- unter behördlicher Aufsicht oder
- wenn dies nach Unionsrecht oder dem Recht eines Mitgliedstaates, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Person vorsieht, zulässig ist.

Die Versicherungswirtschaft ist der Ansicht, dass die Versicherungsaufsicht als eine „behördliche Aufsicht“ i. S. v. Art. 10 DSGVO verstanden werden sollte. In der Kommentarliteratur wird der Begriff jedoch häufig sehr eng verstanden[2].

Vorschlag der deutschen Versicherungswirtschaft:

[2] Z. B. Schwartmann/Jaspers/Thüsing/Kugelmann, Datenschutz-GVO/BDSG, 2. Aufl. 2020, Art. 10 Rn. 4; Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Auflage 2018 Art. 10 Rn. 7.

- **Im BDSG sollte geregelt werden, dass Art. 10 DSGVO der Verarbeitung von Daten über Straftaten und strafrechtliche Verurteilungen nicht entgegensteht, wenn diese zur Erfüllung aufsichtsrechtlicher Anforderungen, im laufenden Versicherungsgeschäft, zur Verhinderung von Betrug oder zur Durchsetzung rechtlicher Ansprüche erforderlich ist. Eine Öffnungsklausel für eine solche Regelung enthält Art. 10 Satz 1 DSGVO.**
- **Sofern davon ausgegangen wird, dass die Versicherungsaufsicht eine „behördliche Aufsicht" i. S. v. Art. 10 DSGVO ist, sollte das BDSG dies zumindest klarstellen.**

4.5. Rechtssicherheit für die Umsetzung der europäischen Digitalstrategie

4.5.1. Anonymisierung und Pseudonymisierung

Der europäische Gesetzgeber verpflichtet Unternehmen, im Rahmen von Vorgaben zum Datenteilen Daten zu anonymisieren, aggregieren oder pseudonymisieren, ohne hierfür eine eindeutige Rechtsgrundlage zu schaffen, z. B. Art. 18 Abs. 5 Data Act. Die deutschen Datenschutzbehörden einschließlich des BfDI vertreten überwiegend die Ansicht, dass die Anonymisierung eine Verarbeitung darstelle und daher einer Rechtsgrundlage bedarf[3], die z. B. der Data Act zumindest ausdrücklich nicht enthält. Selbst wenn man in derartigen Fällen Art. 6 Abs. 1 lit c) oder lit. f) DSGVO als Rechtsgrundlage betrachtet, gilt dies nicht für **besondere Kategorien personenbezogener Daten**. Entgegen dem Erwägungsgrund 50 der DSGVO verstehen die deutschen Datenschutzbehörden auch Art. 6 Abs. 4 DSGVO nur als Erlaubnis für die Zweckänderung, aber nicht als Rechtsgrundlage für die Datenverarbeitung.

Eine Rechtsgrundlage für Anonymisierungen und Pseudonymisierungen zur Erfüllung rechtlicher Verpflichtungen sollte daher in das BDSG aufgenommen werden, damit die Unternehmen, die Anfragen erfüllen müssen, keinem Bußgeld- oder Schadensersatzrisiko ausgesetzt sind. Die Rechtsgrundlage sollte auch Anonymisierungen und Pseudonymisierungen erfassen, die nötig sind, um die Kopien der Daten zu anderen legitimen Zwecken, z. B. zur Entwicklung neuer Anwendungen und Systeme und deren Tests, zu nutzen. Eine Öffnungsklausel für eine solche Regelung enthält für besondere Kategorien personenbezogener Daten Art. 9 Abs. 2 lit. g) DSGVO. Alternativ könnte eine entsprechende Klarstellung in die Gesetzesbegründung, z. B. bei § 24 BDSG, aufgenommen werden.

[3] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Positionspapier zur Anonymisierung unter der DSGVP unter besonderer Berücksichtigung der TK-Branche, 29.06.2020, Pkt. 3., S. 6

Die deutsche Versicherungswirtschaft schlägt vor,

- **eine eindeutige Rechtsgrundlage für die Anonymisierung und Pseudonymisierung von Daten zu schaffen, die auch besondere Kategorien personenbezogener Daten i. S. v. Art. 9 Abs. 1 DSGVO erfasst.**
- **Sofern für die Anonymisierung nach Auffassung der Bundesregierung keine Rechtsgrundlage nötig sein, sollte dies klargestellt werden.**

4.5.2. Entwicklung und Tests von Systemen und Anwendungen

Es existiert bisher keine eindeutige Rechtslage für das Training und Tests von neuen IT-Anwendungen und Systemen mit besonderen Kategorien personenbezogener Daten (z. B. Gesundheitsdaten). Der Vorschlag der EU-Kommission zu einer Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KI-VO) sieht zwar in Art. 10 Abs. 5 eine Rechtsgrundlage vor. Diese beschränkt sich aber leider auf die Entwicklung von hochriskanter KI und gilt nur, soweit dies unbedingt für Zwecke der Verhinderung von Diskriminierungen erforderlich ist. Dieser Ansatz ist ein guter erster Schritt, der in keinem Fall wieder – wie im EU-Parlament gefordert – eingeschränkt werden sollte. Da es im Interesse der Allgemeinheit ist, dass KI- und andere IT-Systeme zu korrekten Ergebnissen kommen, sollten Tests mit pseudonymisierten Echtdaten, inklusive Gesundheitsdaten, zugelassen werden.

Die deutsche Versicherungswirtschaft schlägt vor,

eine eindeutige Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten, insbesondere von besonderen Kategorien nach Art. 9 Abs. 1 DSGVO, für die Entwicklung und Tests von neuen IT-Anwendungen und Systemen zu schaffen.

4.6. Regelungen zu Betroffenenrechten

Dass der deutsche Gesetzgeber die Öffnungsklausel des Art. 23 DSGVO nutzt, ermöglicht eine sachgerechte und verhältnismäßige Anwendung der Regelungen der DSGVO zu den Betroffenenrechten. Die deutsche Versicherungswirtschaft begrüßt die neue ausdrückliche Ausnahme in § 34 Abs. 1 Satz 2 RefE-BDSG (neu) zum Schutz von Betriebs- und Geschäftsgeheimnissen sehr. Darüber hinaus möchten wir auf einige Unstimmigkeiten in den Ausnahmen zu den Betroffenenrechten hinweisen, die im Zuge der aktuellen Änderung des BDSG behoben

werden sollten.

4.6.1. Schutz von Betriebs- und Geschäftsgeheimnissen nach § 34 Abs. 1 Satz 2 RefE-BDSG

Die deutsche Versicherungswirtschaft begrüßt ausdrücklich die Ergänzung des Satzes 2 in § 34 Abs. 1 Satz 2 RefE-BDSG (Artikel 1, Ziffer 10, a), bb)). Damit wird klargestellt, dass das Recht auf Auskunft nach Art. 15 DSGVO auch insoweit nicht besteht, als der betroffenen Person durch die Information ein Betriebs- oder Geschäftsgeheimnis des Verantwortlichen oder eines Dritten offenbart würde und das Interesse an der Geheimhaltung das Interesse der betroffenen Person an der Information überwiegt. Dieses Verständnis lässt sich zwar auch bereits aus § 29 Abs. 1 Satz 2 BDSG herleiten. Durch die Änderung des § 34 BDSG wird aber Rechtssicherheit hergestellt.

4.6.2. Verweis in § 34 Abs. 1 Nr. 1 BDSG auf § 33 Abs. 1 Nr. 2 lit. b) BDSG ergänzen

In § 34 Abs. 1 Nr. 1 BDSG befindet sich derzeit eine **Regelungslücke**. Die Vorschrift sieht zwar eine Ausnahme vom Auskunftsanspruch vor, wenn die betroffene Person nach § 33 Abs. 1 Nr. 2 lit. b) BDSG nicht informiert werden müsste. Es fehlt aber eine entsprechende Ausnahme für § 33 Abs. 1 Nr. 2 lit. a). Danach kann auf eine Information verzichtet werden, wenn diese die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche oder die Verhütung von Schäden durch Straftaten betrifft.

Die Übertragung der Ausnahme von der Informationspflicht auch auf die Auskunftspflicht erscheint sachgerecht und notwendig. So sollte es – z. B. wenn ein Betrug naheliegt – möglich sein, vorerst keine Auskünfte nach Art. 15 DSGVO zu erteilen. Das gilt insbesondere, wenn das Unternehmen noch die Erstattung einer Strafanzeige prüft oder wenn bereits polizeiliche Ermittlungen laufen.

Vorschlag der deutschen Versicherungswirtschaft:

> **Die Verweisung in § 34 Abs. 1 Nr. 1 BDSG sollte sich auch auf § 33 Abs. 1 Nr. 2 lit. a) BDSG erstrecken. Es sollte möglich sein, vorerst keine Auskünfte zu erteilen, wenn dies die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche oder die Verhütung von Schäden durch Straftaten beeinträchtigen würde.**

4.6.3. Übertragung der Ausnahme des § 32 Abs. 2 Satz 3 BDSG in § 33 Abs. 2 BDSG

Eine Unstimmigkeit besteht auch zwischen § 32 Abs. 2 Satz 3 und § 33 Abs. 2 BDSG.
Nach § 32 Abs. 1 Nr. 4 und 5 BDSG kann auf eine Information der Betroffenen nach Art. 13 DSGVO verzichtet werden, wenn diese die Verteidigung von Rechtsansprüchen oder die vertrauliche Übermittlung an eine öffentliche Stelle gefährden könnte. Für diese Fälle sieht § 32 Abs. 2 Satz 3 BDSG vor, dass auch die Pflichten zur Information der Öffentlichkeit und die Dokumentationspflicht nach § 32 Abs. 2 Satz 1 und 2 BDSG nicht gelten. Dies würde nämlich die Zwecke dieser Ausnahmen unterlaufen.

In § 33 Abs. 2 BDSG, der sich auf die vergleichbaren Ausnahmen von der Informationspflicht nach Art. 14 DSGVO in § 33 Abs. 1 Nr. 2 a) und b) BDSG bezieht, fehlt jedoch eine entsprechende Ausnahme. Es gibt keinen Grund, warum hier Pflichten zur Information der Öffentlichkeit und die Dokumentationspflicht bestehen sollten. Vielmehr ist die Interessenlage bei der Information nach Art. 13 und Art. 14 DSGVO gleich, sodass die Regelung des § 32 Abs. 2 Satz 3 BDSG in § 33 Abs. 2 BDSG übertragen werden sollte.

Vorschlag der Versicherungswirtschaft:

> **Die in § 32 Abs. 2 Satz 3 BDSG getroffene Regelung zum Verzicht auf Maßnahmen wie einer Information der Öffentlichkeit in besonderen Fällen, sollte in § 33 Abs. 2 BDSG übernommen werden.**

Berlin, den 6. September 2023