

Positionspapier

des Gesamtverbandes der
Deutschen Versicherungswirtschaft
Lobbyregister-Nr. R000774

zur Modernisierung und Entbürokratisierung des Daten-
schutzrechts in Deutschland

Einleitung

Die Pläne der Bundesregierung, das Datenschutzrecht zu entbürokratisieren, verständlicher zu gestalten und insbesondere die Rechtsunsicherheit für Unternehmen zu reduzieren, werden von der Versicherungswirtschaft ausdrücklich begrüßt.

Die Versicherungswirtschaft bringt mit diesem Positionspapier konkrete Verbesserungsvorschläge ein, wie eine nationale Datenschutzreform aussehen kann, die zugleich das Datenschutzniveau wahrt, wirtschaftliche Prozesse erleichtert und die digitale Wettbewerbsfähigkeit Deutschlands stärkt.

In der täglichen Praxis zeigt sich, dass nicht allein die DSGVO für bürokratische Lasten sorgt, sondern insbesondere ihre restriktive und teils divergierende Auslegung durch deutsche Datenschutzaufsichtsbehörden. Die fragmentierte behördliche Auslegungspraxis sowie die mangelnde Abstimmung zwischen den



**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
Abteilung Recht/Compliance/
Verbraucherschutz

E-Mail

data-protection@gdv.de

Landesaufsichten erschweren eine einheitliche und wirtschaftsfreundliche Umsetzung.

Diese Praxis belastet datenverarbeitende Unternehmen überproportional, führt zu Innovationshemmnissen und steht den politischen Zielen von Digitalisierung und Bürokratieabbau entgegen. Gerade stark regulierte Branchen wie die Versicherungswirtschaft erleben täglich, wie verhältnismäßige Lösungen durch pauschale Anforderungen behindert werden – etwa bei der Anwendung von Art. 15 DSGVO, der Verarbeitung besonderer Kategorien personenbezogener Daten oder bei der Nutzung automatisierter Entscheidungsverfahren oder KI.

Vor diesem Grund begrüßt der GDV es auch, dass sich die Bundesregierung mit der Zuständigkeit der Datenschutzbehörden befasst. Allerdings halten wir eine Zuständigkeitskonzentration bei der Bundesdatenschutzbeauftragten (BfDI) nicht für den richtigen Weg. Aus Sicht der Versicherungswirtschaft sollte vielmehr eine länderübergreifende branchenspezifische Zuständigkeitskonzentration für die Versicherungswirtschaft bei einer Landesdatenschutzbehörde festgelegt werden. Die Konzentration von Branchen bei einer Behörde verhindert den Aufbau umfangreicher neuer Kapazitäten und ggf. auch Kompetenzen, wie es bei einer Konzentration der Aufsicht über die gesamte Wirtschaft bei der BfDI notwendig wäre.

1. Thema 1: Zuständigkeitskonzentration bei der Datenschutzaufsicht

Vorschlag:

Es sollte eine länderübergreifende **branchenspezifische Zuständigkeitskonzentration** für die Versicherungswirtschaft **bei einer Landesdatenschutzbehörde** festgelegt werden.

Begründung:

Die Datenschutzaufsicht in Deutschland ist derzeit auf 17 Landesdatenschutzbehörden und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) verteilt. Diese föderale Struktur führt zu erheblichen Herausforderungen und Ineffizienzen, die insbesondere Unternehmen betreffen.

Unterschiedliche Interpretationen der Datenschutzvorschriften durch die verschiedenen Landesdatenschutzbehörden führen zu Rechtsunsicherheit und erschweren die Umsetzung der Datenschutzgesetze. Insbesondere Unternehmen mit Niederlassungen in mehreren Bundesländern sehen sich mit einer Vielzahl von divergierenden Anforderungen konfrontiert.

Die Genehmigung von brancheneinheitlichen Verfahren durch die deutschen Datenschutzbehörden (z. B. Code of Conduct, Einwilligungserklärungen für die Verarbeitung von Gesundheitsdaten), erfordern die Abstimmung mit 16 Datenschutzaufsichtsbehörden. Es hat sich gezeigt, dass sich solche Abstimmungen meist über mehrere Jahre hinziehen, dies insbesondere auch, da die Behörden sich untereinander auf eine einheitliche Bewertung verständigen müssen.

Eine praktikable Lösung wäre daher, eine länderübergreifende **branchenspezifische Zuständigkeitskonzentration** für die Versicherungswirtschaft **bei einer Landesdatenschutzbehörde** festzulegen.

Dabei sollte die datenschutzrechtliche Aufsicht über alle in Deutschland ansässigen Versicherer von einer Datenschutzaufsichtsbehörde übernommen werden, die aufgrund ihres Standortes bereits über große Erfahrungen in der Beaufsichtigung von Versicherungsunternehmen verfügt (z. B. Bayern oder NRW). Die Konzentration von Branchen bei einer Behörde vermeidet den Aufbau umfangreicher neuer Kapazitäten und ggf. auch Kompetenzen, wie es bei einer Konzentration der Aufsicht über die gesamte Wirtschaft bei der BfDI notwendig wäre. In den Verhandlungen zu den Verhaltensregeln der Versicherungswirtschaft hat sich gezeigt, dass praktikable Lösungen zu einzelnen Fallgestaltungen leichter gefunden werden,

wenn die zuständige Behörde bereits die typischen Abläufe in den Unternehmen der Branche kennt.

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

Vorschlag:

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 und insbesondere auf die Prüfung von Ansprüchen in Regress- und Haftpflichtfällen klargestellt werden.

Begründung:

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 oder zur Prüfung der Regressforderungen von Sozialversicherungsträgern 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. Bei den deutschen Datenschutzbehörden gibt es uneinheitliche Auffassungen dazu. Die Datenschutzbehörden einiger EU-Länder, z. B. Dänemark und Tschechien, wenden ebenfalls Art. 9 Abs. 2 lit. f) DSGVO an.

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.

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 sechs Jahre an. In der Zwischenzeit hatte sogar eine Datenschutzbehörde die Einwilligung als unfreiwillig angegriffen.¹ Wenn sich diese Ansicht verfestigen würde, könnte nicht einmal mehr auf diese Weise Rechtssicherheit erzielt werden.

Die unklare Rechtslage führt auch 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 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 zur Durchführung von Versicherungsverträgen würde für deutsche Erst- und Rückversicherer die dringend benötigte Rechtsklarheit schaffen und langwierige Abstimmungen entbehrlich machen. Sie würde den Datentransfer zur Abwicklung des Versicherungsgeschäfts auf europäischer Ebene erleichtern und Standortnachteile deutscher Erst- und Rückversicherer verhindern. 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.

Hilfreich wäre aber auch schon eine Klarstellung im BDSG, dass die Verarbeitung von Gesundheitsdaten, die zur Durchführung von Versicherungsverträgen (einschließlich der Rückversicherung, der Schadenregulierung in der Haftpflichtversicherung sowie der Einschaltung von Gutachtern) erforderlich ist, nach Art. 9 Abs. 2 lit. f) DSGVO als Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche stets – auch unabhängig von einer streitigen Auseinandersetzung – erlaubt ist.

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.

3. Anpassung der Ausnahmen für automatisierte Entscheidungen in der Versicherungswirtschaft (§ 37 BDSG)

Vorschlag:

§ 37 Abs. 1 und Abs. 2 BDSG sollten vollautomatisierte Entscheidungen im Rahmen des Abschlusses und der Durchführung von Versicherungsverträgen ermöglichen.

Begründung:

Im Zuge zunehmender Digitalisierung müssen Versicherer in der Lage sein, vollautomatisiert über Anträge auf Versicherungsschutz und Leistungen aus Versicherungsverträgen zu entscheiden. Damit kann dem Begehren der Kunden, die eine schnelle Bearbeitung ihrer Anliegen erwarten, besser Rechnung getragen werden.

Beispiele:

- Ein Antrag auf Abschluss eines Lebensversicherungsvertrages mit Gesundheitsangaben wird vom Versicherungsvermittler bei seinem Gespräch mit dem Kunden elektronisch aufgenommen und direkt an das Versicherungsunternehmen geleitet. Dieses prüft den Antrag automatisiert und teilt dem Vermittler noch während des Gesprächs mit, dass der Vertrag angenommen wird. Der Vermittler informiert den Kunden sofort darüber.
- Ein Kunde möchte schnell und unkompliziert eine Unfall- oder Risikolebensversicherung abschließen. Der Versicherer bietet hierfür Online-Abschlüsse mit nur sehr wenigen Gesundheitsfragen an. Der Kunde erwartet den Vertragsschluss (ggf. auch unter Ausschluss von Schäden aufgrund einer bestehenden Erkrankung) noch während der laufenden Online-Sitzung.
- 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 den beiden zuerst genannten Beispielen wären nach § 37 BDSG keine vollautomatisierten Entscheidungen möglich, weil § 37 BDSG das Antragsverfahren nicht abdeckt. Im dritten Beispiel wäre ebenfalls keine vollautomatisierte Entscheidung möglich, weil dem Begehren nicht im Sinne von § 37 Abs. 1 Nr. 1 vollumfänglich stattgegeben wird und der in Nr. 2 genannte Sonderfall nicht vorliegt.

Die in Art. 22 DSGVO enthaltenen Ausnahmen werden von den Datenschutzbehörden sehr eng ausgelegt. Die Behörden betrachten vollautomatisierte Entscheidungen als grundsätzlich nicht „erforderlich“ für den Versicherungsvertrag, wenn nicht eine zeitliche Komponente besteht, welche eine objektive Dringlichkeit der Entscheidung bedingt. Eine Einwilligung sehen die Behörden 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 Datenschutzbehörden nicht aus.

Dem Bedarf könnte 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.

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

Vorschlag:

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 aufgenommen werden. Sofern davon ausgegangen wird, dass die Versicherungsaufsicht eine „behördliche Aufsicht“ i. S. v. Art. 10 DSGVO ist, sollte das BDSG dies klarstellen.

Begründung:

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, 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 an der 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. Die deutschen Datenschutzbehörden legen den Begriff der Aufsicht hier sehr eng aus, und sind der Ansicht, dass die BaFin keine Aufsichtsbehörde i. S. d. Art. 10 DSGVO sei.

Rechtssicherheit würde eine eindeutige Rechtsgrundlage im BDSG schaffen. Dort 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.

5. Rechtsgrundlage für Anonymisierungen und Pseudonymisierungen

Vorschlag:

Es sollte eine Rechtsgrundlage für Anonymisierungen und Pseudonymisierungen zur Erfüllung rechtlicher Verpflichtungen in das BDSG aufgenommen werden, damit die Unternehmen bei der Erfüllung rechtlicher Verpflichtungen keinem Bußgeld- oder Schadensersatzrisiko ausgesetzt sind.

Begründung:

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 der BfDI vertreten überwiegend die Ansicht, dass die Anonymisierung eine Verarbeitung darstelle und daher einer Rechtsgrundlage bedarf, 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 ErwG 50 DSGVO verstehen die deutschen Datenschutzbehörden auch Art. 6 Abs. 4 DSGVO nur als Erlaubnis für die Zweckänderung, aber nicht als Rechtsgrundlage für die Datenverarbeitung.

Es sollte daher eine Rechtsgrundlage für Anonymisierungen und Pseudonymisierungen zur Erfüllung rechtlicher Verpflichtungen in das BDSG aufgenommen werden, damit die Unternehmen bei der Erfüllung rechtlicher Verpflichtungen 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.

Berlin, den 28.10.2025

Ansprechpartner:

Datenschutz/Grundsatzfragen

Abteilung Recht/Compliance/Verbraucherschutz

E-Mail:

data-protection@gdv.de