GDV Gesamtverband der Versicherer

STELLUNGNAHME

Stellungnahme

des Gesamtverbandes der
Deutschen Versicherungswirtschaft
Lobbyregister-Nr. R000774
Transparenzregister-Nr. 6437280268-55

zur Evaluierung der Datenschutz-Grundverordnung (DSGVO)

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

Inhalt

Zusammenfassung

Seit Inkrafttreten der DSGVO haben sich die Anforderungen an die Datenverarbeitung verändert. Die fortschreitende **Digitalisierung** der Geschäftsprozesse erfordert Anpassungen der Regelungen und deren Interpretation durch die Datenschutzbehörden.

- Das Verbot **automatisierter Einzelfallentscheidungen** (Art. 22 DSGVO) mit seinen zu engen Ausnahmen wird der Digitalisierung im Massengeschäft der Versicherer und den Wünschen der Kunden nach einer schnellen Bearbeitung ihrer Anliegen nicht mehr gerecht. Um diesen geänderten Bedürfnissen besser zu entsprechen, wäre aus unserer Sicht statt eines Verbots eine Kombination aus anderen, aber sehr effektiven Schutzinstrumenten besser geeignet: Transparenz über die automatisierte Entscheidung und – auf Wunsch der Kunden – vertiefte Informationen zur Entscheidungsfindung und Überprüfbarkeit durch einen Menschen. Zumindest sollten die einschränkende Auslegung der Ausnahmen durch die Datenschutzbehörden aufgegeben und weitere Ausnahmen für die Regulierung von Ansprüchen Dritter geschaffen werden (siehe dazu Ziffer 2.1).
- Die Anforderungen an die **Anonymisierung** personenbezogener Daten sollten definiert werden sowie klar und leicht erfüllbar sein (2.2).
- IT-Anwendungen, Produkte, Systeme und Analysemodelle können zwar oft mit synthetischen oder anonymisierten Daten entwickelt werden. Um sie sicher und diskriminierungsfrei in Betrieb zu nehmen, sind Tests mit echten personenbezogenen Daten oft notwendig. Es bedarf dazu über Art. 10 Abs. 5 KI-VO hinaus einer eindeutigen Rechtsgrundlage für die Nutzung personenbezogener Daten, einschließlich besondere Kategorien, soweit dies für die **Entwicklung** und für **Tests** von IT-Anwendungen, Produkten, Systemen und Analysemodellen zwingend erforderlich ist. Dabei sollte dem Schutz der Rechte und Interessen der betroffenen Personen durch hohe technische und organisatorische Maßnahmen genügt werden (2.3).
- Der Grundsatz der **Datenminimierung** ist im Hinblick auf selbstlernende Systeme überholt (2.4).
- In Bezug auf die **Datenübermittlung in Drittstaaten** (Art. 44 ff. DSGVO) sollten technische und organisatorische Maßnahmen risikobasiert getroffen werden können. Ferner sollten die Anforderungen an Binding Corporate Rules (BCRs) und Einwilligungen in die Datenübermittlung in Drittstaaten auf das gesetzlich geforderte Maß beschränkt werden (2.5).

Bei der Anwendung der DSGVO hat sich darüber hinaus weiterer Handlungsbedarf gezeigt.

- Eine **europaweit einheitliche Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten in der Versicherungsbranche** würde die Rechtssicherheit erhöhen und ein Level-Playing-Field für Erst- und Rückversicherer in Europa schaffen (3.1).

- Für die **Datenverarbeitung in Unternehmensgruppen**, insbesondere von Daten i. S. v. Art. 9 DSGVO, sollte eine eindeutige Rechtsgrundlage geschaffen werden (3.2).
- Die **Betroffenenrechte** sollten dem datenschutzrechtlichen Risiko entsprechen. Informationspflichten können gegenüber Geschäftspartnern und ihren Mitarbeitenden und entsprechend dem Kontext der Verarbeitung eingeschränkt werden (3.3.1). Auskunftsrechte sollten auf ihren datenschutzrechtlichen Zweck begrenzt werden (3.3.2).
- Die Entwicklung branchen- und verarbeitungsspezifischer **Codes of Conduct** sollte effektiver gefördert werden (3.4).

1. Einleitung

Die deutschen Versicherungsunternehmen verwalten mehr als 450 Mio. Versicherungsverträge. Sie regulieren Schäden und erbringen Leistungen in Höhe von jährlich mehr als 180 Mrd. Euro. Seit Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) hat sich die Datenverarbeitung in den Unternehmen massiv verändert. **Verarbeitungsprozesse** werden immer weiter **digitalisiert**. Die EU-Kommission hat die Bedeutung von Daten für die Wettbewerbsfähigkeit der europäischen Wirtschaft erkannt und **zahlreiche Gesetzgebungsvorhaben zur Verbesserung des Datenaustausches** angestoßen. Die meisten dieser Gesetze lassen die DSGVO unberührt, was allerdings zu großen Herausforderungen bei der Anwendung dieser Gesetze führt, wie z. B. beim Data Act, dem European Health Data Space und bei der Financial Data Access Regulation.

Das Datenschutzrecht muss jedoch auch in der Lage sein, mit diesen Entwicklungen mitzuhalten. In vielen Fällen lassen sich die Bestimmungen der DSGVO durchaus „digitalisierungsfreundlich“ interpretieren. Jedoch erhalten sie durch **Leitlinien des EDSA** oftmals ein deutlich engeres Verständnis, das durch die Auslegung der nationalen Datenschutzbehörden schließlich zum **Digitalisierungs- und damit Innovationshemmnis** wird.

In der Stellungnahme zeigen wir datenschutzrechtliche Digitalisierungshemmnisse auf und unterbreiten Vorschläge, wie diese ausgeräumt werden könnten. Ferner erläutern wir den Bedarf für spezielle **Rechtsgrundlagen** für die Datenverarbeitung in der Versicherungswirtschaft, für die Einschränkung überbordender **Betroffenenrechte** sowie für die Förderung der Implementierung von **Codes of Conduct**.

2. Datenschutz als Digitalisierungshemmnis

2.1 Automatisierte Einzelfallentscheidungen (Art. 22 DSGVO)

Kunden der Versicherungsunternehmen erwarten eine immer schnellere Bearbeitung und Entscheidung ihrer Versicherungsangelegenheiten, insbesondere bei Online-Vertragsabschlüssen und Online-Schadenmeldungen. Ohne automatisierte Einzelfallentscheidungen ist diese Anforderung nicht mehr zu erfüllen. Die in Art. 22 DSGVO geregelten automatisierten Einzelfallentscheidungen gewinnen folglich im täglichen Geschäft von Versicherungen stetig zunehmend an Relevanz.

Es hat sich gezeigt, dass Art. 22 DSGVO in seiner aktuellen Fassung, nicht zuletzt aufgrund seiner Interpretation durch die Datenschutzbehörden und den EuGH, der Digitalisierung zu enge Grenzen setzt.

Der EuGH hat in seinem Urteil vom 07.12.2023 in der Rechtssache „C-634/21 - SCHUFA Holding (Scoring)“ Art. 22 DSGVO ausdrücklich als **Verbotsnorm** bezeichnet. Das bedeutet, dass eine unter die Norm fallende automatisierte Einzelfallentscheidung rechtswidrig ist, wenn nicht eine Ausnahme nach Art. 22 Abs. 2 oder Abs. 4 DSGVO einschlägig ist.

Die in Art. 22 Abs. 2 und Abs. 4 DSGVO geregelten **Ausnahmen** von dem Verbot werden von den Datenschutzaufsichtsbehörden **über Ihren Wortlaut hinaus eng ausgelegt**. Zudem **fehlen Ausnahmen** für praktisch relevante Sachverhalte. Damit werden automatisierte Einzelfallentscheidungen, die im täglichen Massengeschäft von Versicherungsunternehmen sehr sinnvoll wären, stark eingeschränkt.

Zu enge Auslegung der Ausnahmen in Art. 22 Abs. 2 und 4 DSGVO

Der Europäische Datenschutzausschuss und nationale Datenschutzaufsichtsbehörden schränken die in Art. 22 Abs. 2 und Abs. 4 DSGVO geregelten Ausnahmen über Ihren Wortlaut hinaus ein.

Nach Ansicht des EDSA soll eine automatisierte Einzelfallentscheidung nach **Art. 22 Abs. 2 lit a) DSGVO** nur dann für den Abschluss oder die Erfüllung eines Vertrages „erforderlich“ im Sinne der Norm sein, wenn das angestrebte Ziel nicht mit einer datenschutzfreundlicheren Lösung erreicht werden kann (Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, WP 251 rev.01 Ziff. IV.C.1.). Die deutschen Datenschutzbehörden folgern daraus, dass eine vollautomatisierte Entscheidungsfindung für die Erfüllung eines Versicherungsvertrages in der Regel nicht „erforderlich“ ist, da diese Aufgabe auch von Menschen wahrgenommen werden kann.

Die Datenschutzbehörden sind ferner der Ansicht, dass eine wirksame Einwilligung nach **Art. 22 Abs. 2 lit. c), Art. 22 Abs. 4, Art. 7 Abs. 4 DSGVO** nur dann gegeben werden kann, wenn die betroffene Person von Anfang an die Möglichkeit hat, anstelle der vollautomatisierten Entscheidungsfindung die Verarbeitung durch einen Menschen zu wählen. Sie stützen dies auf die Leitlinien 05/2020 des EDSA zu Einwilligungen (Rn. 30). Damit wird die unternehmerische Freiheit, digitale Produkte anzubieten, übermäßig beschränkt.

Diese enge Auslegung der Ausnahmen läuft darauf hinaus, dass Kundenangelegenheiten in Unternehmen nicht einmal in einem ersten (später überprüfbaren) Durchlauf vollständig automatisiert bearbeitet werden können. Die Digitalisierung von Prozessabläufen wird damit entweder ganz verhindert oder es werden den Unternehmen organisatorische Maßnahmen aufgebürdet, die den Vorteil der Digitalisierung wieder zunichtemachen.

Fehlende Ausnahme für Ansprüche Dritter

Die in Art. 22 Abs. 2 und Abs. 4 DSGVO geregelten **Ausnahmen** decken nicht alle in der Praxis relevanten Datenverarbeitungen ab.

Beispiel:

> Schäden in der Haftpflichtversicherung, z. B. bei Kfz-Unfällen, können auf der Basis von Online-Angaben oft vollautomatisiert geprüft und damit schnell reguliert werden.

Auf die automatisierten Einzelfallentscheidungen eines Versicherungsunternehmens gegenüber geschädigten Personen in der Haftpflichtversicherung ist Art. 22 Abs. 2 lit a) DSGVO aber schon nach seinem Wortlaut nicht anwendbar. Denn die Geschädigten sind nicht Vertragspartner des Versicherungsunternehmens. Die Einholung der Einwilligung stößt auf noch größere Schwierigkeiten als im Vertragsverhältnis, da der Geschädigte nur seinen Anspruch auf Schadensersatz geltend macht und keine vertragliche Beziehung zwischen ihm und dem Versicherungsunternehmen des Schädigers besteht.

Ausnahme von Entscheidungen, soweit dem Begehren stattgegeben wird

Es ist immer noch unsicher, ob Entscheidungen, die dem Begehren der betroffenen Person stattgeben, von Art. 22 DSGVO erfasst sind.

Beispiel:

> Ein Versicherungsunternehmen nimmt einen Antrag auf Abschluss eines Versicherungsvertrages an oder es zahlt die Leistung, die ein Versicherungsnehmer

fordert, nach vollautomatisierter Prüfung des Schadenfalls an den Anspruchsteller aus.

Derartige Entscheidungen entfalten „rechtliche Wirkung“ und scheinen daher – auf den ersten Blick betrachtet – vom Wortlaut des Art. 22 Abs. 1 DSGVO erfasst zu sein. Anhaltspunkte, dass sie dennoch vom Anwendungsbereich ausgeschlossen sind, ergeben sich nur durch Auslegung der Norm. So folgert der Generalanwalt in seinen Schlussanträgen in der Rechtssache C 634/21 aus der anderen im Gesetz vorgesehenen Alternative „oder ihn in ähnlicher Weise erheblich beeinträchtigt“, dass Art. 22 insgesamt nur „schwerwiegende Auswirkungen“ erfassen soll (Rn. 34). Eine Klarstellung in Art. 22 Abs. 1 DSGVO oder eine eindeutige Ausnahme würde Rechtssicherheit schaffen.

Transparenz und Überprüfbarkeit als bessere Schutzmechanismen

Das Verbot automatisierter Einzelentscheidungen mit den zu engen Ausnahmen führt dazu, dass Entscheidungen, die schnell und unkompliziert automatisiert getroffenen werden könnten, Menschen überlassen werden müssen. Die Folge sind Zeitverzögerungen und höhere Kosten, die letztlich zu Beitragssteigerungen für die Versicherungsnehmer führen.

Dass ein Verbot nicht mehr zeitgemäß ist, zeigen auch Art. 6 ff. KI-Verordnung, die selbst hochriskante KI nicht untersagen, sondern Transparenz und Überprüfbarkeit vorsehen.

Die Rechte und Interessen der betroffenen Personen könnten auch im Rahmen des Art. 22 DSGVO effektiv sichergestellt werden. Bei der Mitteilung der Entscheidung sollte Transparenz darüber geschaffen werden, dass die Entscheidung vollautomatisiert getroffen wurde. Ferner sollten Rechte der betroffenen Personen bestehen, auf Verlangen die wesentlichen Gründe für die Entscheidung zu erfahren, den eigenen Standpunkt darzulegen, die Entscheidung anzufechten und eine Überprüfung durch eine natürliche Person auf Seiten des Verantwortlichen zu bewirken.

Vorschläge der deutschen Versicherungswirtschaft:

⇒ Damit Art. 22 DSGVO der fortschreitenden Digitalisierung gerecht werden kann, sollte die Regelung **nicht mehr als Verbot** ausgestaltet werden. Automatisierte Einzelfallentscheidungen sollten grundsätzlich möglich sein. Die **Rechte und Interessen der betroffenen Personen** könnten sichergestellt werden durch Transparenz, dass die Entscheidung vollautomatisiert getroffen wurde, und das Recht, die wesentlichen Gründe für die Entscheidung zu erfahren, die Entscheidung anzufechten und eine Überprüfung durch eine natürliche Person zu erhalten.

Mindestens sollten folgende Maßnahmen getroffen werden:

- ⇒ Es sollte durch weitere Präzisierungen sichergestellt werden, dass die in Art. 22 Abs. 2 und 4 DSGVO geregelten Ausnahmen nicht mehr durch die einschränkenden Interpretationen der Datenschutzbehörden leerlaufen.
- ⇒ Eine weitere Ausnahme sollte auch für die Regulierung von Ansprüchen betroffener Personen, die nicht Vertragspartner des Verantwortlichen sind, geschaffen werden (Beispiel: Geschädigter Dritter in der Haftpflichtversicherung). Ihre Rechte und Interessen würden auch hier – wie im ersten Absatz beschrieben – sichergestellt.
- ⇒ Im Gesetzestext sollte rechtssicher klargestellt werden, dass automatisierte Einzelfallentscheidungen vom Anwendungsbereich des Art. 22 DSGVO ausgenommen sind, soweit dem Begehren der betroffenen Person stattgegeben wird.

2.2 Anonymisierung von Daten

Neue Rechtsakte der EU zum Austausch von Daten erfordern die Anonymisierung von Daten, wie z. B. Art. 18 Abs. 5 Data Act für die Datenübermittlung an öffentliche Stellen. Eine Anonymisierung personenbezogener Daten ist auch für viele Datenanalysen nötig, die im Rahmen der Digitalisierung eine immer größere Rolle spielen. Auch um bestehende Anwendungen weiterzuentwickeln sowie neue Anwendungen, Produkte und Systeme zu trainieren und zu testen, werden so lange wie möglich anonymisierte Daten eingesetzt. Es besteht jedoch eine erhebliche Rechtsunsicherheit darüber, wann Daten hinreichend anonymisiert sind, zumal der EDSA die hierzu angekündigten Leitlinien bisher noch nicht herausgegeben hat.

Werden Daten nur dann als anonym betrachtet, wenn niemand sie einer Person zuordnen kann, ist praktisch keine Anonymisierung denkbar. Daher ist das Europäische Gericht in seinem Urteil vom 26.04.2023 (T-557/20) zu Recht von einem relativen Ansatz bei der Bestimmung der Personenbeziehbarkeit ausgegangen. Kritisch ist auch, dass einige Datenschutzbehörden für die Anonymisierung von Daten eine Rechtgrundlage nach Art. 6 und ggf. nach Art. 9 DSGVO verlangen. Eine gute Anonymisierung ist aber einer Löschung vergleichbar, die im Interesse des Datenschutzes wünschenswert ist. Das wird auch in Erwägungsgrund 26 Satz 5 und 6 zur DSGVO deutlich. Sie sollte daher keiner Rechtsgrundlage bedürfen.

Vorschläge der deutschen Versicherungswirtschaft:

- ⇒ Unternehmen benötigen rechtssichere, verlässliche Regelungen, wann Daten hinreichend anonymisiert sind und nicht mehr der DSGVO unterliegen.
- ⇒ Der Personenbezug von Daten sollte relativ bestimmt werden. Entscheidend ist,

dass derjenige, der die Daten verarbeitet, sie keiner bestimmten Person zuordnen kann.

⇒ Es sollte klargestellt werden, dass die Anonymisierung von Daten keine Erlaubnisgrundlage nach Art. 6 und ggf. 9 DSGVO erfordert.

2.3 Entwicklung und Tests von IT-Anwendungen, Produkten und Systemen

Es liegt im Interesse der Allgemeinheit, dass IT-Anwendungen, Produkte, Systeme und Analysemodelle mit echten personenbezogenen Daten sicher funktionieren und zu korrekten Ergebnissen kommen. Das gilt vor allem, wenn besondere Kategorien personenbezogener Daten verarbeitet werden sollen, wie z. B. Gesundheitsdaten in der Lebens- und Krankenversicherung. Zwar können im Anfangsstadium der Entwicklung oft synthetische oder anonymisierte Daten verwendet werden. Um Datensicherheit zu gewährleisten und unerwünschte Ergebnisse auszuschließen, sind allerdings zumindest abschließend, manchmal aber auch schon im Entwicklungsstadium, Tests mit Echtdaten nötig. Zudem stellt sich bei Big-Data-Anwendungen das Problem, dass keine ausreichende Menge von synthetischen Testdaten vorhanden ist, sodass auf Echtdaten zurückgegriffen werden muss. Schließlich bestehen immer Unsicherheiten, ob eine Anonymisierung hinreichend ist (dazu 2.2).

Beispiele:

> Nach der Entwicklung und Integrationstestung von neuen IT-Anwendungen werden vor deren Inbetriebnahme in einer produktionsnahen Umgebung Last- und Performance-Tests mit echten Datensätzen durchgeführt. Dabei werden die Daten pseudonymisiert, soweit es im Hinblick auf den konkreten Anwendungsfall möglich und sinnvoll ist.
>
> Intelligente Anwendungen werden in abgesicherten Testumgebungen daraufhin überprüft, ob sie Ergebnisse produzieren, die der Realität entsprechen. Dabei wird der Output mit Ergebnissen verglichen, die in echten Anwendungsfällen auf herkömmliche Weise erzielt wurden.

Es existiert bisher in der DSGVO keine eindeutige Rechtsgrundlage für die Datenverarbeitung zur Entwicklung und zum Test von IT-Anwendungen, Produkten, Systemen und Analysemodellen mit besonderen Kategorien personenbezogener Daten i. S. v. Art. 9 Abs. 1 DSGVO. Insbesondere in Deutschland fordern Datenschutzbehörden (entgegen dem eindeutigen Wortlaut von Erwägungsgrund 50 Satz 2) neben Art. 6 Abs. 4 DSGVO eine weitere Rechtsgrundlage. Eine Einwilligung der Kunden ist jedoch keine praktikable Lösung. Sie bedeutet nicht nur bürokratischen Aufwand. Da die Kunden keinen unmittelbar spürbaren Vorteil von den Tests haben, sind auf entsprechende Anfragen kaum Rückmeldungen zu erwarten.

Art. 10 Abs. 5 der KI-VO zeigt, dass der Gesetzgeber das Problem erkannt hat. Jedoch sieht die Norm nur für einen eng begrenzten Fall eine Rechtsgrundlage für Tests mit Echtdaten vor. Sie beschränkt sich auf die Entwicklung hochriskanter KI und gilt nur, soweit dies unbedingt für Zwecke der Verhinderung von Diskriminierungen erforderlich ist. Um die Anforderungen der DSGVO an die Datensicherheit erfüllen zu können und bei Live-Schaltung der Anwendungen und Systeme keine fehlerhaften Ergebnisse und Datenpannen zu riskieren, muss auch in allen anderen Fällen der Einsatz von echten Datensätzen im Entwicklungs- und Teststadium möglich sein.

Was in der KI-Verordnung für hochriskante KI zugelassen wird, sollte erst recht für weniger riskante Datenverarbeitung mit Daten nach Art. 9 Abs. 1 DSGVO möglich sein.

Entscheidend ist, dass zum Schutz der Rechte und Interessen der betroffenen Personen ausreichende Vorkehrungen getroffenen werden. Dazu gehören eine Beschränkung der Nutzung von echten personenbezogenen Daten auf das unbedingt erforderliche Maß sowie technische und organisatorische Maßnahmen, um eine hohe Datensicherheit zu gewährleisten. Das können z. B. eine enge Begrenzung der Zugriffsrechte, ein hoher Schutz der Vertraulichkeit und Integrität der Daten und – sofern möglich – eine Pseudonymisierung oder Verschlüsselung sein.

Vorschlag der deutschen Versicherungswirtschaft:

⇒ In die DSGVO sollte eine eindeutige Erlaubnisgrundlage für die Verarbeitung von personenbezogenen Daten, einschließlich besonderer Kategorien, aufgenommen werden, soweit dies für die Entwicklung und Tests von neuen IT-Anwendungen, Produkten und Systemen zwingend erforderlich ist. Zum Schutz der Rechte und Interessen der betroffenen Personen sollten technische und organisatorische Maßnahmen, z.B. eine enge Begrenzung der Zugriffsrechte, ein hoher Schutz der Vertraulichkeit und Integrität der Daten und - sofern möglich - eine Pseudonymisierung oder Verschlüsselung vorgesehen werden.

2.4 Datenminimierung

Zielrichtung der Digitalisierungsgesetzgebung in Europa ist ein verbesserter Austausch und damit die bessere Nutzbarkeit von Daten. Im Interesse der Allgemeinheit sollen mehr und bessere Erkenntnisse aus den Daten gewonnen werden. Insbesondere wenn Daten mittels selbstlernender KI-Anwendungen ausgewertet werden, kann der Umfang der von der KI verwendeten Daten nicht immer von vornherein abgesehen werden. Damit steht es im Widerspruch, die Datenverarbeitung auf ein Minimum zu beschränken. Somit entstehen zwangsläufig Konflikte mit dem **Grundsatz der Datenminimierung** nach Art. 5 Abs. 1 lit. c) DSGVO.

Der Grundsatz steht auch dem – von den Gesetzgebern der KI-VO intendierten – Ziel der Verhinderung von Diskriminierungen entgegen. Die Erfahrung hat gezeigt, dass Diskriminierung häufig dann auftrat, wenn die Datenbasis veraltet oder vergleichsweise gering war. Dem kann begegnet werden, indem man mit einer möglichst großen und ungefilterten Datenbasis operiert.

Vorschlag der deutschen Versicherungswirtschaft:

⇒ Die EU-Kommission sollte eine Lockerung des Grundsatzes der Datenminimierung ins Auge fassen.

2.5 Erleichterung der Datenübermittlung in Drittstaaten

In einer vernetzten Welt ist es für Unternehmen kaum noch möglich, ihre Datenverarbeitung auf das Gebiet der EU zu beschränken. Daher müssen rechtssichere Instrumente für die Datenübermittlung in Drittstaaten zur Verfügung stehen.

Das EU-US-Privacy-Framework und die aktuelle Bestätigung der bereits getroffenen Angemessenheitsbeschlüsse für weitere Drittstaaten sind Schritte in die richtige Richtung. Für andere Drittstaaten, wie z. B. Indien und Brasilien, fehlen jedoch noch entsprechende Beschlüsse. Es ist wünschenswert, dass die EU-Kommission die Angleichung der Jurisdiktionen in weiteren Staaten aktiv unterstützt, um weitere Angemessenheitsbeschlüsse fassen zu können.

Ungeachtet dessen sind jetzt Lösungen nötig, um den Datenverkehr rechtskonform zu ermöglichen.

2.5.1 Risikobasierter Ansatz in Art. 44 ff. DSGVO und Hilfestellungen zur Einschätzung der Rechtslage in Drittstaaten

Die Verwendung der überarbeiteten Standarddatenschutzklauseln reicht nach der Schrems-II-Rechtsprechung des EuGH nicht aus, um eine Datenübermittlung in Drittstaaten zu rechtfertigen. Der EDSA hat im Anschluss an die Schrems-II-Rechtsprechung mit den Empfehlungen 1/2020 sehr hohe Anforderungen an Datenübermittlungen in Drittstaaten gestellt. Unternehmen haben erheblichen Aufwand, da sie in jedem Einzelfall das Datenschutzniveau im Drittland prüfen und ggf. zusätzliche Schutzmaßnahmen treffen müssen. Die nationalen Datenschutzbehörden halten die Datenübermittlung im Ergebnis oft selbst dann für unzulässig, wenn es um Daten mit geringem Schutzbedarf geht und das Risiko für einen Zugriff auf die Daten gering ist (z. B. Übermittlung beruflicher E-Mail-Adressen anlässlich einer Videokonferenz). Es ist nicht nachvollziehbar, warum der in der DSGVO angelegte risikobasierte Ansatz (Art. 24 und 32 DSGVO) nicht auf die zur

Datenübermittlung in Drittstaaten getroffenen technischen und organisatorischen Maßnahmen angewandt werden soll.

Vorschläge der deutschen Versicherungswirtschaft:

⇒ Die EU-Kommission sollte die Anwendung des risikobasierten Ansatzes (Art. 24 und 32 DSGVO) auf die zur Datenübermittlung in Drittstaaten getroffenen Maßnahmen ausdrücklich in den Art. 44 ff. DSGVO verankern.
⇒ Zur Einschätzung der Rechtslage in Drittstaaten wären zudem Hilfestellungen der EU-Kommission sinnvoll.

2.5.2 Binding Corporate Rules

Binding Corporate Rules im Sinne von Art. 47 DSGVO sind grundsätzlich ein sinnvolles Instrument für Datenübermittlungen in Drittstaaten innerhalb von Konzernen. Mit den Empfehlungen 1/2022 hat der EDSA die Anforderungen, die bis dahin an Controller Binding Corporate Rules (BCRs) gestellt wurden (vgl. WP 256 und WP 264 der Art.-29-Datenschutzgruppe) bereits nach kurzer Geltungsdauer deutlich erweitert. Den Empfehlungen zufolge müssen die BCR-Regelungen nun praktisch die gesamten Anforderungen der DSGVO abbilden. Darüber hinaus müssen sie eine Vielzahl zusätzlicher Maßnahmen vorsehen, die die Anforderungen des Art. 47 DSGVO übersteigen. Die Erweiterungen gehen damit erheblich über das hinaus, was die Umsetzung der Schrems-II-Rechtsprechung erfordert. Vor allem macht die lange Dauer des Genehmigungsprozesses in der Praxis BCRs als Instrument für Datenübermittlungen in Drittländer für Konzerne zunehmend unattraktiv.

Vorschlag der deutschen Versicherungswirtschaft:

⇒ Die EU-Kommission sollte sich dafür einsetzen, dass die Anforderungen an BCRs auf das von Art. 47 DSGVO geforderte Maß zurückgeführt und die Genehmigungsprozesse verkürzt werden.

2.5.3 Weniger strenge Auslegung der Ausnahmen in Art. 49 DSGVO

Unter den Voraussetzungen des Art. 49 DSGVO sind Datenübermittlungen in Drittstaaten auch ohne die in Art. 46 DSGVO genannten Garantien möglich. So erlaubt Art. 49 Abs. 1 lit. a) DSGVO Datenübermittlungen auf der Grundlage der ausdrücklichen **Einwilligung** der betroffenen Person, nachdem sie über die möglichen Risiken solcher Übermittlungen informiert wurde. Die Anforderungen an die Transparenz gehen über die allgemeinen Transparenzanforderungen an Einwilligungen nach Art. 6 Abs. 1 lit. a) bzw. Art. 9 Abs. 2 lit a) i. V. m. Art. 7 DSGVO ausdrücklich hinaus und erfassen die besondere

Risikosituation. Weder im Wortlaut noch in den Erwägungsgründen wird die Einwilligungsmöglichkeit darüber hinaus eingeschränkt. Dennoch lassen die Datenschutzbehörden die Einwilligung für Datenübermittlungen in Drittstaaten nur im Ausnahmefall zu. Dies widerspricht dem Recht auf informationelle Selbstbestimmung, das aus Art. 8 EMRK abgeleitet wird.

Vorschlag der deutschen Versicherungswirtschaft:

⇒ Die EU-Kommission sollte dafür Sorge tragen, dass Datenübermittlungen in Drittstaaten nicht über den Wortlaut das Art. 49 DSGVO hinaus eingeschränkt werden.

3. Weiterer Änderungsbedarf

3.1 Verarbeitung von Gesundheitsdaten in der Versicherungsbranche

Die private Lebens-, Kranken- und Unfallversicherung ersetzt teils die gesetzliche Sozialversicherung (z. B. die substitutive Krankenversicherung in Deutschland) und bietet außerdem wichtige Ergänzungen der gesetzlichen Sozialversicherung. Verträge in der Lebens-, Kranken- und Unfallversicherung können nur abgeschlossen und durchgeführt werden, wenn Gesundheitsdaten verarbeitet werden. Gleiches gilt in der Haftpflicht- und Rechtsschutzversicherung, wenn Ansprüche wegen Gesundheitsschäden geltend gemacht werden. Die Rechtslage in Bezug auf die Verarbeitung dieser Gesundheitsdaten in der privaten Versicherungswirtschaft ist aber unsicher. Datenschutzbehörden lehnen einerseits eine Anwendung des Art. 9 Abs. 2 lit. f) DSGVO sowie anderer für die Sozialversicherung in Art. 9 Abs. 2 DSGVO vorgesehener Ausnahmen ab. Andererseits stellen sie in der Praxis kaum erfüllbare Anforderungen an die Freiwilligkeit von Einwilligungen. Manche europäischen Länder haben nationale Rechtsgrundlagen für die Datenverarbeitung geschaffen, die im Einzelnen voneinander abweichen. Die Situation führt zu praktischen Schwierigkeiten im grenzüberschreitenden Datenverkehr. So erhalten z. B. Rückversicherer, die selbst keinen direkten Kundenkontakt haben, nur schwer eine Einwilligung für ihre Datenverarbeitung in Ländern, in denen die Erstversicherer keine Einwilligung benötigen. Generell ist eine Einwilligung keine hinreichend verlässliche und effiziente Rechtsgrundlage für die Erfüllung eines Versicherungsvertrags, weil sie jederzeit widerrufen werden kann.

Vorschlag der deutschen Versicherungswirtschaft:

⇒ Eine eindeutige gesetzliche Erlaubnisgrundlage für die Datenverarbeitung zum Abschluss und zur Durchführung von Versicherungsverträgen (einschließlich der Rückversicherung) in Art. 9 Abs. 2 DSGVO würde die dringend benötigte Rechtssicherheit für Erst- und Rückversicherer in allen europäischen Ländern gleichermaßen und ein Level-Playing-Field für alle europäischen Versicherer schaffen.

3.2 Datenverarbeitung im Konzern

Um Synergien zu erzielen und dem Gebot der Wirtschaftlichkeit zu entsprechen, werden innerhalb von Versicherungsgruppen – ebenso wie in Gruppen anderer Branchen – Aufgaben delegiert und zentralisiert. Dies ist versicherungsaufsichtsrechtlich gemäß Art. 38, 49 der Richtlinie 2009/138/EG und Art. 274 der Verordnung (EU) 2015/35 zulässig.

Beispiel:

> Die Konzernmutter oder eine Dienstleitungsgesellschaft übernimmt die Risikoprüfung und Schadensbearbeitung für alle Gesellschaften der Unternehmensgruppe, zu denen ein Krankenversicherer, ein Lebensversicherer und ein Kompositversicherer mit Unfallsparte gehören.

Ist eine Datenverarbeitung im Konzern keine Auftragsverarbeitung nach Art. 28 DSGVO, liegt rechtlich eine Datenübermittlung an einen Dritten vor. Art. 6 Abs. 1 lit. f) DSGVO rechtfertigt aber nicht die Verarbeitung besonderer Kategorien personenbezogener Daten und kommt insofern als Rechtsgrundlage nicht in Betracht. Die Einholung einer Einwilligung bei allen Kunden wäre unpraktikabel und während der Laufzeit eines Versicherungsvertrages kaum Erfolg versprechend. Die Rückmeldungen von Kunden bewegen sich erfahrungsgemäß in solchen Fällen im einstelligen Prozentbereich.

Vorschlag der deutschen Versicherungswirtschaft:

⇒ Für eine rechtssichere Datenverarbeitung in Unternehmensgruppen, insbesondere von besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO, sollte in der DSGVO eine eindeutige Rechtsgrundlage geschaffen werden.

3.3 Risikobasierter Ansatz bei den Betroffenenrechten

Informations- und Auskunftsrechte sind wichtige Instrumente, um dem Datenschutz Geltung zu verschaffen. Hohe bürokratische Anforderungen bewirken jedoch das Gegenteil.

3.3.1 Informationspflichten (Art. 13, 14 DSGVO)

Bei der Anwendung der DSGVO hat sich früh gezeigt, dass die umfangreichen Informationspflichten nach Art. 13, 14 DSGVO den Bedürfnissen im Geschäftsverkehr nicht gerecht werden und zu unnötigen Belastungen der betroffenen Personen und der Unternehmen führen. Das gilt nicht nur für kleine und mittlere Unternehmen.

Beispiele:

> In der geschäftlichen Kommunikation und im geschäftlichen Schriftverkehr erwarten die Geschäftspartner und deren Mitarbeiter keine Datenschutzinformation.
>
> Beim telefonischen Erstkontakt mit Kunden und Anspruchstellern werden die „Verlesung“ der Datenschutzinformationen und selbst der Hinweis in aller Regel als lästige Verzögerung empfunden.

Der vom EDSA in den Leitlinien für Transparenz gemäß der Verordnung 2016/679 (WP 260 rev.01, Rn. 35f) eingeführte Mehrebenen-Ansatz (Layered Approach) bringt nur eine geringfügige Erleichterung, weil die auf erster Ebene zu liefernden Informationen noch immer umfangreich sind.

Vorschläge der deutschen Versicherungswirtschaft:

⇒ Zur Vermeidung von unnötigem Bürokratieaufwand und einer Überflutung von betroffenen Personen mit Informationen sollten die in Art. 13, 14 DSGCO vorgesehenen Angaben im B2B-Bereich gegenüber Geschäftspartnern und deren Mitarbeitern nur elektronisch vorgehalten werden müssen.
⇒ Im übrigen Geschäftsverkehr sollten sich die Erforderlichkeit, die Art und Weise, der Umfang und der Zeitpunkt proaktiv zu liefernder Information risikobasiert nach dem Kontext der Datenverarbeitung richten. Wenn nach den Umständen typischerweise keine Information erwartet wird, sollte die Information nicht proaktiv, sondern ebenfalls elektronisch vorgehalten und nur auf Anforderung zugesendet werden müssen.

3.3.2 Auskunftsrecht (Art. 15 DSGVO)

Versicherungsunternehmen speichern im Rahmen des laufenden Geschäfts zahlreiche personenbezogene Daten über ihre Kunden, Versicherungsvermittler und Mitarbeiter (z. B. Schadenfälle, eingereichte Rechnungen, Courtage-Abrechnungen, im Namen der Unternehmen geführte Korrespondenz). Es hat sich in der Praxis gezeigt, dass der Auskunftsanspruch nach Art. 15 DSGVO vermehrt nicht nur zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung (vgl. ErwGr. 63) genutzt wird.

Beispiel:

> Bei Streitigkeiten mit dem Versicherungsunternehmen setzt ein ehemaliger Mitarbeiter oder Kunde seinen Auskunftsanspruch als Druckmittel ein und fordert Auskunft über alle Mails, die an ihn gerichtet waren, und alle Unterlagen, in denen er erwähnt ist.

Der EuGH legt Art. 15 DSGVO (Az. C-307/22) sehr weit aus, in dem er eine Auskunftspflicht auch dann bejaht, wenn diese datenschutzfremden Zwecken dient. Auch die Interpretation durch den EDSA in den Leitlinien 1/2022 ist weit.

Der Auskunftsanspruch geht nach dieser Interpretation weit über den Schutzzweck des Datenschutzrechts hinaus. Nach ErwGr. 63, Satz 1 DSGVO dient er dazu, dass sich die betroffene Person einen Überblick über die durch den Verantwortlichen durchgeführte Verarbeitung ihrer personenbezogenen Daten machen und die Rechtmäßigkeit der Verarbeitung prüfen kann. Es ist in der DSGVO dagegen nicht vorgesehen, dass der Auskunftsanspruch zur Beweiserlangung, als Druckmittel oder zur Erleichterung des eigenen Dokumentenmanagements genutzt werden kann. Der datenschutzrechtliche Auskunftsanspruch sollte dem Schutzzweck des Datenschutzrechts gerecht werden und nicht zu außerhalb des Schutzzwecks der DSGVO liegenden Zwecken missbraucht werden können.

Vorschläge der deutschen Versicherungswirtschaft:

⇒ Der Zweck des datenschutzrechtlichen Auskunftsanspruchs, die Überprüfung ordnungsgemäßer Datenverarbeitung, sollte ausdrücklich in Art. 15 DSGVO verankert werden.
⇒ Zwecke, zu denen keine Auskunft verlangt werden kann, z. B. die Geltendmachung zur Umgehung der Beweislastverteilung im Zivilprozess, der Einsatz als Druckmittel oder Schikane, sollten als Regelbeispiele für ein nicht bestehendes Auskunftsrecht in Art. 15 oder Art. 12 Abs. 5 DSGVO aufgenommen werden.

3.4 Förderung von Codes of Conduct

Art. 40 DSGVO sieht Verhaltensregeln zur Konkretisierung der DSGVO vor. Diese Codes of Conduct können die allgemeinen Bestimmungen der DSGVO branchen- oder verarbeitungsbereichsspezifisch konkretisieren. Sie bieten damit sowohl für Unternehmen als auch für die Datenschutzaufsichtsbehörden eine gute Orientierung, um die Rechtmäßigkeit der Datenverarbeitung zu beurteilen. Gemäß Art. 46 Abs. 2 lit. e) i. V. m. Art. 40 Abs. 3 DSGVO können Verhaltensregeln zudem geeignete Garantien für die Datenübermittlung in Drittstaaten bieten. Von dieser sinnvollen Lösung wird bisher in der Praxis kaum Gebrauch gemacht. Dies liegt vor allem daran, dass die in den Leitlinien 1/2019 des EDSA festgeschriebenen Anforderungen an Verhaltensregeln und deren Überwachung die Vorgaben in Art. 40 und 41 DSGVO übersteigen und nur mit erheblichem Aufwand umzusetzen sind. Die Leitlinien des EDSA bieten zudem Auslegungsspielraum, der die nationalen Datenschutzbehörden dazu veranlasst, die Anforderungen noch weiter zu erhöhen bzw. aufgrund von Unsicherheiten Genehmigungsverfahren zu verzögern.

Beispiel:

> Einige Datenschutzbehörden vertreten die Ansicht, dass ein Code of Conduct neben den Bestimmungen, die die DSGVO branchenspezifisch konkretisieren, keinerlei ergänzende Bestimmungen, die die DSGVO wiedergeben, enthalten darf, auch wenn dies dem besseren Verständnis der Datenverarbeitung in der Branche dienen würde.

Vorschlag der deutschen Versicherungswirtschaft:

⇒ Die Kommission sollte dem in Art. 40 Abs. 1 DSGVO verankerten Auftrag, die Entwicklung von Codes of Conduct zu fördern, aktiv nachkommen und dafür Sorge tragen, dass keine über Art. 40, 41 DSGVO hinausgehenden Anforderungen gestellt werden.

Berlin, den 27.03.2024