Version Stand: 10.10.2025

Verhaltensregeln
für den Umgang mit personenbezogenen Daten
durch die deutsche Versicherungswirtschaft

Inhalt

I. EINLEITUNG 2

II. BEGRIFFSBESTIMMUNGEN 4

III. ALLGEMEINE BESTIMMUNGEN 6
Art. 1 Geltungsbereich 6
Art. 2 Zwecke der Verarbeitung 7
Art. 3 Grundsätze der Datensicherheit 7
Art. 4 Transparenz 8
Art. 5 Einwilligung 8
Art. 6 Besondere Kategorien personenbezogener Daten 9

IV. VERARBEITUNG PERSONENBEZOGENER DATEN 10
Art. 7 Grundsätze zur Datenerhebung und Informationen bei Datenerhebung bei der betroffenen Person 10
Art. 8 Datenerhebung bei anderen Stellen als den betroffenen Personen (Datenerhebung bei Dritten) 10
Art. 9 Verarbeitung von Stammdaten in der Unternehmensgruppe 11
Art. 10 Statistik, Tarifkalkulation und Prämienberechnung 12
Art. 11 Scoring 14
Art. 12 Bonitätsdaten 14
Art. 13 Automatisierte Einzelentscheidungen 14
Art. 14 Hinweis- und Informationssystem (HIS) 16
Art. 15 Aufklärung von Widersprüchlichkeiten 17
Art. 16 Datenaustausch mit anderen Versicherern 18
Art. 17 Datenübermittlung an Rückversicherer 19

V. VERARBEITUNG PERSONENBEZOGENER DATEN FÜR VERTRIEBSZWECKE UND ZUR MARKT- UND MEINUNGSFORSCHUNG 20
Art. 18 Verwendung von Daten für Zwecke der Werbung 20
Art. 19 Marktumfragen 20
Art. 20 Datenübermittlung an selbstständige Vermittler 21

VI. DATENVERARBEITUNG DURCH AUFTRAGSVERARBEITER, DIENSTLEISTER UND GEMEINSAM VERANTWORTLICHE 22
Art. 21 Pflichten bei der Verarbeitung im Auftrag 22
Art. 22 Datenverarbeitung durch eigenverantwortliche Dienstleister 22

Art. 22a Gemeinsam verantwortliche Stellen 24

VII. RECHTE DER BETROFFENEN PERSONEN 24
Art. 23 Auskunftsanspruch 24
Art. 24 Recht auf Datenübertragbarkeit 25
Art. 25 Löschung 26

VIII. EINHALTUNG UND KONTROLLE 26
Art. 26 Verantwortlichkeit 26
Art. 27 Datenschutz-Folgenabschätzung 26
Art. 28 Datenschutzbeauftragte 27
Art. 29 Beschwerden und Reaktion bei Verstößen 27

IX. ÜBERWACHUNG DER EINHALTUNG DER VERHALTENSREGELN 28
Art. 29a Überwachungsstelle 28
Art. 29b Personelle Ausstattung, Zuverlässigkeit und fachliche Eignung 28
Art. 29c Unabhängigkeit und Vermeidung von Interessenkonflikten 29
Art. 29d Allgemeine Aufgaben und Befugnisse der Überwachungsstelle 30
Art. 29e Beschwerdebearbeitung 30
Art. 29f Geeignete Maßnahmen der Überwachungsstelle bei Verstößen 31
Art. 29g Vertraulichkeit 32
Art. 29h Dokumentation und Unterrichtung 32
Art. 29i Substanzielle Veränderungen 33
Art. 29j Finanzierung der Überwachung 33
Art. 29k Verfahrensordnung 33

X. FORMALIA 33
Art. 30 Beitritt 33
Art. 31 Evaluierung 34
Art. 32 Inkrafttreten 34

I. EINLEITUNG

Der Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) mit Sitz in Berlin ist die Dachorganisation der privaten Versicherer in Deutschland. Ihm gehören über 450 Mitgliedsunternehmen an. Diese bieten als Risikoträger Risikoschutz und Unterstützung sowohl für private Haushalte als auch für Industrie, Gewerbe und öffentliche Einrichtungen. Der Verband setzt sich für alle die Versicherungswirtschaft betreffenden Fachfragen und für ordnungspolitische Rahmenbedingungen ein, die den Versicherern die optimale Erfüllung ihrer Aufgaben ermöglichen.

Die Versicherungswirtschaft ist von jeher darauf angewiesen, in großem Umfang personenbezogene Daten der Versicherten zu verwenden. Sie werden zur Antrags-, Vertrags- und Leistungsabwicklung verarbeitet, um Versicherte zu beraten und zu betreuen. Es gilt das zu versichernde Risiko einzuschätzen, die Leistungspflicht zu prüfen und Versicherungsmissbrauch im Interesse der Versichertengemeinschaft zu verhindern. Versicherungen können dabei heute ihre Aufgaben nur noch mit Hilfe der elektronischen Datenverarbeitung erfüllen.

Die Wahrung der informationellen Selbstbestimmung und der Schutz der Privatsphäre sowie die Sicherheit der Datenverarbeitung sind für die Versicherungswirtschaft ein Kernanliegen, um das Vertrauen der Versicherten zu gewährleisten. Alle Regelungen zur Verarbeitung personenbezogener Daten müssen nicht nur im Einklang mit den Bestimmungen der Europäischen Datenschutz-Grundverordnung (DSGVO), des Bundesdatenschutzgesetzes (BDSG) und aller einschlägigen bereichsspezifischen Vorschriften über den Datenschutz stehen, sondern die diesen Verhaltensregeln beigetretenen Unternehmen der Versicherungswirtschaft verpflichten sich darüber hinaus, den Grundsätzen der Transparenz, der Erforderlichkeit der verarbeiteten Daten und der Datenminimierung in besonderer Weise nachzukommen.

Hierzu hat der GDV im Einvernehmen mit seinen Mitgliedsunternehmen die folgenden Verhaltensregeln für den Umgang mit den personenbezogenen Daten der Versicherten aufgestellt. Sie schaffen für die Versicherungswirtschaft weitestgehend einheitliche Standards und fördern die Einhaltung von datenschutzrechtlichen Regelungen. Unternehmen, die die brancheninternen Verhaltensregeln anwenden, stellen damit sicher, dass die Vorgaben der DSGVO für die Versicherungswirtschaft branchenspezifisch konkretisiert werden. Die Mitgliedsunternehmen des GDV, die diesen Verhaltensregeln gemäß Artikel 30 beigetreten sind, verpflichten sich damit zu deren Einhaltung.

Die Verhaltensregeln sollen den Versicherten der beigetretenen Unternehmen die Gewähr bieten, dass Datenschutz- und Datensicherheitsbelange bei der Gestaltung und Bearbeitung von Produkten und Dienstleistungen berücksichtigt werden. Der GDV versichert seine Unterstützung bei diesem Anliegen. Die beigetretenen Unternehmen weisen ihre Führungskräfte und ihre Mitarbeiterinnen und Mitarbeiter an, die Verhaltensregeln einzuhalten. Antragsteller und Versicherte werden über die Verhaltensregeln informiert.

Darüber hinaus sollen die Verhaltensregeln verdeutlichen, welche Datenverarbeitungen in der Regel auf gesetzlicher Grundlage oder auf Basis von Einwilligungserklärungen zulässig sind. Grundsätzlich sind Einwilligungen nur noch für die Verarbeitung von besonderen Kategorien personenbezogener Daten – wie Gesundheitsdaten – sowie für die Verarbeitung personenbezogener Daten zu Zwecken der Werbung erforderlich.

Die vorliegenden Verhaltensregeln konkretisieren und präzisieren die gesetzlichen datenschutzrechtlichen Regelungen für die Versicherungsbranche. Als konkretisierende und präzisierende Regelungen für die beigetretenen Mitgliedsunternehmen des GDV erfassen sie wichtige Verarbeitungen personenbezogener Daten, welche die Unternehmen im Zusammenhang mit der Begründung, Durchführung, Beendigung oder Akquise von Versicherungsverträgen sowie zur Erfüllung gesetzlicher Verpflichtungen vornehmen. Daneben gibt es in den Unternehmen weitere Verarbeitungen personenbezogener Daten auf gesetzlicher Grundlage. Die einschlägigen gesetzlichen Bestimmungen, die für die jeweilige Verarbeitungssituation gelten, werden durch die vorliegenden Verhaltensregeln nicht ersetzt und bleiben daher stets anwendbar. Soweit diese mit anderen Worten wiedergegeben werden, ist rechtlich maßgeblich letztlich allein der Gesetzestext.

Da die Verhaltensregeln geeignet sein müssen, die Datenverarbeitung aller beigetretenen Unternehmen zu regeln, sind sie möglichst allgemeingültig formuliert. Deshalb kann es erforderlich sein, dass die einzelnen Unternehmen diese in unternehmensspezifischen Regelungen weiter konkretisieren. Das mit den Verhaltensregeln erreichte Datenschutz- und Datensicherheitsniveau wird dabei nicht unterschritten. Darüber hinaus ist es den Unternehmen unbenommen, Einzelregelungen, z. B. für besonders sensible Daten wie Gesundheitsdaten oder für die Verarbeitung von Daten im Internet, zu treffen. Haben die beigetretenen Unternehmen bereits besonders datenschutzfreundliche Regelungen getroffen oder bestehen mit den zuständigen Datenschutzaufsichtsbehörden spezielle Vereinbarungen oder Absprachen zu datenschutzgerechten Verfahrensweisen, behalten diese selbstverständlich auch nach dem Beitritt zu diesen Verhaltensregeln ihre Gültigkeit.

Unbeschadet der hier getroffenen Regelungen gelten die Vorschriften der DSGVO und des BDSG sowie anderer einschlägiger Rechtsvorschriften über den Datenschutz oder mit datenschutzrechtlicher Wirkung. Selbstverständlich werden alle Betroffenenrechte beachtet, auch wenn diese im Folgenden nicht explizit erwähnt werden. Der Beschäftigtendatenschutz ist nicht Gegenstand dieser Verhaltensregeln.

II. BEGRIFFSBESTIMMUNGEN

Für die Verhaltensregeln gelten die Begriffsbestimmungen der DSGVO und des Bundesdatenschutzgesetzes.

Darüber hinaus sind im Sinne dieser Verhaltensregeln:

Antragsteller:
Personen, die ein Angebot angefragt haben oder einen Antrag auf Abschluss eines Versicherungsvertrages stellen, unabhängig davon, ob der Versicherungsvertrag zustande kommt.

Auftragsverarbeiter:
eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

automatisierte Entscheidung:
eine Entscheidung gegenüber einer einzelnen Person, die auf eine ausschließlich automatisierte Verarbeitung gestützt wird, ohne dass eine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat.

betroffene Personen:
Versicherte, Antragsteller oder weitere Personen, deren personenbezogene Daten im Zusammenhang mit dem Versicherungsgeschäft verarbeitet werden.

Bezugsberechtigte:
Personen, die entsprechend der Bestimmung des Versicherungsnehmers in der privaten Renten-, Lebens- oder Unfallversicherung die vereinbarten Leistungen im Versicherungsfall oder bei regulärem Ablauf der Versicherung erhalten.

Datenschutzbeauftragte/r:
der oder die von dem Versicherungsunternehmen benannte Datenschutzbeauftragte im Sinne von § 38 Bundesdatenschutzgesetz und Kapitel IV. Abschnitt 4 der DSGVO.

Dienstleister:
andere Unternehmen oder Personen, die als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO Aufgaben für das Unternehmen wahrnehmen.

Geschädigte:
Personen, die einen Schaden erlitten haben oder erlitten haben könnten, wie z. B. Anspruchsteller in der Haftpflichtversicherung.

schutzwürdige Interessen:
Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Stammdaten:
die allgemeinen Daten der betroffenen Personen: Name, Adresse, Geburtsdatum, Geburtsort, Kundennummer, Beruf, Familienstand, gesetzliche Vertreter, Angaben über die Art der bestehenden Verträge (wie Vertragsstatus, Beginn- und Ablaufdaten, Versicherungsnummer(n), Zahlungsart, Rollen der betroffenen Person (z. B. Versicherungsnehmer, versicherte Person, Beitragszahler, Anspruchsteller) sowie Kontoverbindung, Telekommunikationsdaten, Authentifizierungsdaten für die elektronische oder telefonische Kommunikation, Werbesperren und andere Widersprüche, Werbeeinwilligung und Sperren für Markt- und Meinungsforschung, Vollmachten und Betreuungsregelungen, zuständige Vermittler und mit den genannten Beispielen vergleichbare Daten.

Unternehmen:
die Mitgliedsunternehmen des GDV, soweit sie das Versicherungsgeschäft als Erstversicherer betreiben sowie mit diesem in einer Gruppe von Versicherungs- und Finanzdienstleistungsunternehmen verbundene Erstversicherungsunternehmen, einschließlich Pensionsfonds, die diesen Verhaltensregeln beigetreten sind.

Vermittler:
selbstständig handelnde natürliche Personen (Handelsvertreter) und Gesellschaften, welche als Versicherungsvertreter oder -makler im Sinne des § 59 Versicherungsvertragsgesetz (VVG) Versicherungsverträge vermitteln oder abschließen.

Versicherungsgeschäft:
nach der ständigen Rechtsprechung des Bundesverwaltungsgerichts, wenn gegen Entgelt für den Fall eines ungewissen Ereignisses bestimmte Leistungen übernommen werden, wobei das übernommene Risiko auf eine Vielzahl durch die gleiche Gefahr bedrohter Personen verteilt wird und der Risikoübernahme eine auf dem Gesetz der großen Zahl beruhende Kalkulation zugrunde liegt. Dazu gehören alle zur Anbahnung, Erfüllung und Abwicklung von Versicherungsverträgen notwendigen geschäftlichen Tätigkeiten und innerbetriebliche Leistungen wie die Bestandsverwaltung und Leistungsbearbeitung, die Kundenberatung, die Produktgestaltung, Tarifierung und Prämienberechnung sowie die Marktforschung, das Rechnungswesen, die interne Revision, die Vermögensanlage und die Vermögensverwaltung inklusive aller dafür erforderlichen Datenverarbeitungen.

Versicherungssparte (Sparte):

eine Zusammenfassung von Versicherungszweigen bzw. Versicherungsgeschäften eines Versicherungsunternehmens, die separiert von anderen Versicherungszweigen bzw. Versicherungsgeschäften in einer eigenen Rechtseinheit zu betreiben sind. In Deutschland werden die Sparten Lebensversicherung, private Krankenversicherung und Schaden-/Unfallversicherung (synonym: Kompositversicherung) unterschieden, wobei letztere die Gesamtheit aller übrigen Versicherungszweige ist. Üblicherweise wird die Rückversicherung ebenfalls als eine Versicherungssparte bezeichnet.

Versicherungsverhältnis:

Versicherungsvertrag einschließlich der damit im Zusammenhang stehenden vorvertraglichen Maßnahmen und rechtlichen Verpflichtungen.

Versicherte:

- Versicherungsnehmer und Versicherungsnehmerinnen des Unternehmens,
- versicherte Personen einschließlich der Teilnehmer an Gruppenversicherungen.

weitere Personen:

außerhalb des Versicherungsverhältnisses stehende Personen, wie Geschädigte, Zeugen und sonstige Personen, deren Daten das Unternehmen im Zusammenhang mit der Begründung, Durchführung oder Beendigung eines Versicherungsverhältnisses verarbeitet.

Wissenschaftliche Forschung:

jede geistige Tätigkeit mit dem Ziel, in methodischer, systematischer sowie nachprüfbarer Art und Weise neue Erkenntnisse zu gewinnen. Die bloße Anwendung bereits gewonnener Erkenntnisse fällt demgegenüber ebenso wenig unter den Begriff der wissenschaftlichen Forschung wie der Einsatz wissenschaftlicher Methoden zu reinen Aufsichts-, Kontroll-, Organisations- oder Werbezwecken. Dabei sind im Sinne einer methodischen und systematischen Vorgehensweise fachspezifische Eigenarten und Besonderheiten zur Ermittlung der rationalen Wahrheit zu berücksichtigen. Die Nachprüfbarkeit der Forschungsergebnisse ist möglichst durch deren Veröffentlichung, im Falle von im Einzelfall entgegenstehenden schutzwürdigen Betriebs- oder Geschäftsgeheimnissen jedenfalls aber durch eine nach wissenschaftlichen Standards erstellte Dokumentation der Durchführung und der Ergebnisse des Forschungsvorhabens, die einer wissenschaftlichen Überprüfung standhalten kann, sicherzustellen. Die forschende Stelle oder Einheit im Unternehmen arbeitet unabhängig gegenüber anderen Stellen oder Bereichen des Unternehmens, so dass diese keinen erheblichen Einfluss auf die Durchführung oder die Ergebnisse nehmen können. Die Forschung dient vornehmlich dem Gemeinwohl, auch wenn das Verfolgen begleitender wirtschaftlicher Motive nicht die wissenschaftliche Forschung im Sinne der DSGVO ausschließt, solange die Tätigkeit auf Erzielung eines gesellschaftlichen Nutzens gerichtet ist.

III. ALLGEMEINE BESTIMMUNGEN

Art. 1 Geltungsbereich

[1]Die Verhaltensregeln gelten für die Verarbeitung personenbezogener Daten im Zusammenhang mit dem Versicherungsgeschäft durch die Unternehmen. [2]Dazu gehört neben dem Ver-

sicherungsverhältnis insbesondere die Erfüllung gesetzlicher Ansprüche, auch wenn ein Versicherungsvertrag nicht zustande kommt, nicht oder nicht mehr besteht. [3]Zum Versicherungsgeschäft gehören auch die Gestaltung und Kalkulation von Tarifen und Produkten.

Art. 2 Zwecke der Verarbeitung

[1]Die Verarbeitung personenbezogener Daten erfolgt für die Zwecke des Versicherungsgeschäfts, soweit dies zur Begründung, Durchführung und Beendigung von Versicherungsverhältnissen erforderlich ist, insbesondere zur Bearbeitung eines Antrags, zur Beurteilung des zu versichernden Risikos, zur Erfüllung der Beratungspflichten nach dem Versicherungsvertragsgesetz (VVG), zur Prüfung einer Leistungspflicht und zur internen Prüfung des fristgerechten Forderungsausgleichs. [2]Sie erfolgt insbesondere auch zur Prüfung und Regulierung der Ansprüche Geschädigter in der Haftpflichtversicherung, zur Prüfung und Abwicklung von Regressforderungen, zum Abschluss und zur Durchführung von Rückversicherungsverträgen, zur Entwicklung von Tarifen, Produkten und Services, zur Erstellung von Statistiken, für versicherungsrelevante Forschungszwecke, z. B. Unfallforschung, zur Missbrauchsbekämpfung oder zur Erfüllung gesetzlicher und aufsichtsrechtlicher Verpflichtungen oder zu Zwecken der Werbung sowie der Markt- und Meinungsforschung.

Art. 3 Grundsätze der Datensicherheit

(1) [1]Zur Gewährleistung der Datensicherheit werden die erforderlichen technisch-organisatorischen Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. [2]Dabei werden angemessene Maßnahmen getroffen, die insbesondere gewährleisten können, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen und verarbeiten können (Vertraulichkeit). Mittel hierzu sind insbesondere Berechtigungskonzepte, Pseudonymisierung oder Verschlüsselung personenbezogener Daten.

2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität, Richtigkeit).

3. personenbezogene Daten auch in Fällen von internen und externen Störungen oder Lastspitzen zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit, Belastbarkeit).

4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität).

5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise eingegeben, übermittelt und verändert hat (Revisionsfähigkeit).

6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

(2) [1]Die in den Unternehmen veranlassten Maßnahmen werden in ein umfassendes, die Verantwortlichkeiten regelndes Datenschutz- und -sicherheitskonzept integriert, welches

unter Einbeziehung der Datenschutzbeauftragten erstellt wird. [2]Es beinhaltet insbesondere Verfahren zur regelmäßigen Überprüfung und Bewertung der Wirksamkeit der getroffenen Maßnahmen und ein Konzept für den Umgang mit Verletzungen des Schutzes personenbezogener Daten. [3]Die Unternehmen legen darin fest, dass alle Verletzungen des Schutzes personenbezogener Daten den Datenschutzbeauftragten zur Kenntnis zu geben sind.

Art. 4 Transparenz

(1) [1]Texte, die sich an betroffene Personen richten, werden informativ, transparent, verständlich und präzise sowie in klarer und einfacher Sprache formuliert. [2]Sie werden den betroffenen Personen in leicht zugänglicher Form zur Verfügung gestellt.

(2) Informationen über den Beitritt zu diesen Verhaltensregeln sowie weitere Informationen, die nach diesen Verhaltensregeln in geeigneter Form bekannt zu geben sind (Artikel 9 Abs. 3 Satz 3, Artikel 21 Abs. 3 Satz 4, Artikel 22 Abs. 8 Satz 3, Artikel 22a Abs. 2 Satz 1 Artikel 27 Abs. 3 Satz 3, Artikel 28 Abs. 1 Satz 3, Artikel 29e Abs. 3 Satz 2 und Artikel 30 Abs. 1 Satz 2 und Abs. 3 Satz 3), werden im Internet veröffentlicht; in jedem Fall werden sie auf Anfrage in einer der Anfrage entsprechenden Textform (Brief, Kundenportal, E-Mail u. a.) zugesandt.

(3) [1]Von einer Verletzung des Schutzes personenbezogener Daten betroffene Personen werden benachrichtigt, wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für ihre persönlichen Rechte und Freiheiten zur Folge hat. [2]Dies erfolgt unverzüglich. [3]Vorrangig und als Voraussetzung der Benachrichtigung sind Maßnahmen zur Untersuchung der Ursache und der Auswirkung sowie zur Behebung bzw. Eindämmung der Verletzung zu ergreifen. [4]Würde eine Benachrichtigung unverhältnismäßigen Aufwand erfordern, z. B. wegen der Vielzahl der betroffenen Fälle oder wenn eine Feststellung der betroffenen Personen nicht in vertretbarer Zeit oder mit vertretbarem technischem Aufwand möglich ist, tritt an ihre Stelle eine Information der Öffentlichkeit oder eine ähnliche Maßnahme.

Art. 5 Einwilligung

(1) [1]Soweit die Verarbeitung personenbezogener Daten auf eine Einwilligung sowie – soweit erforderlich – auf eine Schweigepflichtentbindungserklärung der betroffenen Personen gestützt wird, stellt das Unternehmen sicher, dass diese freiwillig, in informierter Weise und unmissverständlich bekundet wird, wirksam und nicht widerrufen ist. [2]Soweit besondere Kategorien personenbezogener Daten – insbesondere Daten über die Gesundheit – verarbeitet werden, muss die diesbezügliche Einwilligung für einen oder mehrere festgelegte Zwecke ausdrücklich abgegeben sein.

(2) [1]Für die Einholung der Erklärungen nach Absatz 1 ist die Einsichtsfähigkeit maßgeblich. [2]Die Einsichtsfähigkeit eines Minderjährigen für diese Erklärungen ist im Regelfall mit Vollendung des 16. Lebensjahres gegeben. [3]Ist die Einsichtsfähigkeit nicht gegeben, werden die Erklärungen von dem gesetzlichen Vertreter eingeholt. [4]Solange der Minderjährige die Erklärung noch nicht abgegeben hat, bleiben Erklärungen der gesetzlichen Vertreter bestehen. [5]Die zivilrechtlichen Regelungen bleiben unberührt.

(3) [1]Die Einwilligung und die Schweigepflichtentbindung können jederzeit mit Wirkung für die Zukunft ohne Angabe von Gründen widerrufen werden. [2]Die betroffenen Personen werden über die Möglichkeiten und Folgen des Widerrufs einer Einwilligungserklärung

informiert. [3]Mögliche Folge eines wirksamen Widerrufs einer Einwilligungs- und Schweigepflichtentbindungserklärung zur Verarbeitung von Gesundheitsdaten kann insbesondere in der Lebens-, Kranken-, Unfallpflichtversicherung sein, dass ein Antrag auf Leistungsprüfung ab dem Zeitpunkt des Widerrufs nicht mehr bearbeitet und eine Leistung daher nicht erbracht werden kann.

(4) [1]Eine Einwilligung kann schriftlich, elektronisch oder mündlich erteilt werden. [2]Das Unternehmen wird die Erklärung so dokumentieren, dass der Inhalt der jeweils erteilten Einwilligungserklärung nachgewiesen werden kann. [3]Auf Verlangen wird den betroffenen Personen der Erklärungsinhalt zur Verfügung gestellt.

(5) Wird die Einwilligung mündlich eingeholt, ist dies den betroffenen Personen unverzüglich schriftlich oder in Textform zu bestätigen.

Art. 6 Besondere Kategorien personenbezogener Daten

(1) [1]Besondere Kategorien personenbezogener Daten im Sinne der DSGVO (insbesondere Angaben über die Gesundheit) werden auf gesetzlicher Grundlage oder mit Einwilligung der betroffenen Personen (Art. 6 i. V. m. Art. 9 DSGVO) nach Artikel 5 dieser Verhaltensregeln und – soweit erforderlich – aufgrund einer Schweigepflichtentbindung erhoben und verarbeitet.

(2) [1]Die Verarbeitung besonderer Kategorien personenbezogener Daten auf gesetzlicher Grundlage ist zulässig, insbesondere wenn es zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. [2]Ein Anwendungsfall kann die Prüfung und Abwicklung der Ansprüche von Versicherten sowie von Geschädigten in der Haftpflichtversicherung sein. [3]Ein weiterer Anwendungsfall ist regelmäßig die Verarbeitung von Gesundheitsdaten betroffener Personen zur Geltendmachung, Prüfung und Abwicklung von gesetzlich geregelten Regressforderungen einerseits des Unternehmens oder andererseits eines Dritten, der gegenüber der betroffenen Person eine Leistung erbracht hat, wie beispielsweise zur Prüfung und Abwicklung der Regressforderungen eines Sozialversicherungsträgers, Arbeitgebers oder privaten Krankenversicherungsträgers.

(3) Die Verarbeitung besonderer Kategorien personenbezogener Daten kann im Rahmen der gesetzlichen Vorgaben auch dann zulässig sein, soweit es zur Gesundheitsvorsorge bzw. -versorgung erforderlich ist.

(4) [1]Ebenso kann die Verarbeitung von Gesundheitsdaten ohne Einwilligung erfolgen zum Schutz lebenswichtiger Interessen der betroffenen oder anderer Personen, wenn diese aus körperlichen oder rechtlichen Gründen außerstande sind, ihre Einwilligung zu geben.[2]Typische Anwendungsfälle liegen vor, wenn für diese Personen:

- in der Auslandsreisekrankenversicherung schnell eine Kostenübernahme für z. B. die Kosten einer Krankenhausbehandlung im Ausland benötigt wird oder

- Assistance-Leistungen, wie z. B. ein Krankentransport aus dem Ausland oder die Koordination der medizinischen Behandlung, vereinbart sind und diese Leistung schnell benötigt wird

und die betroffenen Personen oder ihre gesetzlichen Vertreter außer Stande sind, ihre Einwilligung abzugeben, z. B. weil sie nach einem Unfall oder einem sonstigen Krankheitsereignis das Bewusstsein nicht wiedererlangt haben oder nicht in der Lage sind, den Inhalt einer Einwilligungserklärung zu erfassen.

(5) [1]Die Verarbeitung besonderer Kategorien personenbezogener Daten erfolgt auch auf gesetzlicher Grundlage zu statistischen Zwecken sowie zu wissenschaftlichen Forschungszwecken nach Maßgabe von Artikel 10 dieser Verhaltensregeln.

IV. VERARBEITUNG PERSONENBEZOGENER DATEN

Art. 7 Grundsätze zur Datenerhebung und Informationen bei Datenerhebung bei der betroffenen Person

(1) Bei der Erhebung personenbezogener Daten von Versicherten und Antragstellern werden die Mitwirkungspflichten nach §§ 19, 31 VVG berücksichtigt.

(2) [1]Personenbezogene Daten weiterer Personen im Sinne dieser Verhaltensregeln werden erhoben und verarbeitet, wenn es zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist. [2]Das gilt insbesondere für die Erhebung von Daten von Zeugen oder von Geschädigten anlässlich einer Leistungsprüfung und -erbringung in der Haftpflichtversicherung und für Datenverarbeitungen zur Erfüllung von Direktansprüchen in der Kfz-Haftpflichtversicherung oder zur Erfüllung von gesetzlichen Meldepflichten. [3]Daten nach Satz 1 können auch erhoben und verarbeitet werden, wenn dies im Zusammenhang mit der Begründung, Durchführung oder Beendigung eines Versicherungsverhältnisses erforderlich ist und die schutzwürdigen Interessen dieser Personen nicht überwiegen, beispielsweise wenn Daten eines Rechtsanwalts oder einer Reparaturwerkstatt zur Korrespondenz im Leistungsfall benötigt werden.

(3) [1]Die Unternehmen stellen sicher, dass die betroffenen Personen zur Gewährleistung der Transparenz und zur Wahrung ihrer Rechte gemäß Art. 13 DSGVO zum Zeitpunkt der Erhebung informiert werden.

Art. 8 Datenerhebung bei anderen Stellen als den betroffenen Personen (Datenerhebung bei Dritten)

(1) [1]Das Unternehmen erhebt personenbezogene Daten nicht nur bei den betroffenen Personen, sondern kann auch bei Dritten personenbezogene Daten erheben, beispielsweise wenn:

- zur Prüfung eines Antrags der betroffenen Person Angaben von Sachverständigen benötigt werden,
- der Versicherungsnehmer bei Gruppenversicherungen zulässigerweise die Daten der versicherten Personen oder bei Lebens- und Unfallversicherungen die Daten der Bezugsberechtigten angibt oder
- in der Haftpflichtversicherung Angaben über Geschädigte oder Zeugen gemacht werden.

[2]Ohne Mitwirkung der betroffenen Person können personenbezogene Daten auch zu Zwecken nach Artikel 10 erhoben werden.

(2) [1]Die Erhebung von Gesundheitsdaten oder genetischen Daten bei Dritten erfolgt – soweit erforderlich – mit wirksamer Schweigepflichtentbindungserklärung der betroffenen Personen und nach Maßgabe des § 213 VVG und § 18 GenDG, soweit diese Vorschriften anzuwenden sind.

(3) [1]Das Unternehmen, das personenbezogene Daten ohne Mitwirkung der betroffenen Personen erhebt, stellt sicher, dass die betroffenen Personen innerhalb einer unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten angemessenen Frist, längstens jedoch innerhalb eines Monats, nach der Erlangung der personenbezogenen Daten gemäß Art. 14 DSGVO informiert werden. [2]Falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, erfolgt die Information zum Zeitpunkt der ersten Offenlegung, es sei denn, dass eine andere gesetzliche Frist kürzer ist. [3]Falls die Daten zur Kommunikation mit den betroffenen Personen verwendet werden sollen, erfolgt die Information spätestens mit der ersten Mitteilung an sie, zum Beispiel in Fällen der Benennung von Bezugsberechtigten in der Lebensversicherung bei Eintritt des Leistungsfalls oder in Fällen der Benennung von Berechtigten für Notfälle, wenn dieser eintritt.

(4) [1]Die Information unterbleibt in den in Art. 14 Abs. 5 DSGVO geregelten Fällen auch, wenn die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen des überwiegenden berechtigten Interesses eines Dritten, geheim gehalten werden müssen. [2]Dies betrifft beispielsweise Fälle in der Lebensversicherung, in denen sich der Versicherungsnehmer wünscht, dass ein Bezugsberechtigter nicht informiert wird.

(5) [1]Ebenso unterbleibt die Information nach Maßgabe des § 33 Abs. 1 Nr. 2 Bundesdatenschutzgesetz in Verbindung mit Art. 23 Abs. 1 lit. j) DSGVO, wenn:

- sie die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde oder die Verarbeitung von personenbezogenen Daten aus zivilrechtlichen Verträgen beinhaltet und der Verhütung von Schäden durch Straftaten dient, sofern nicht das berechtigte Interesse der betroffenen Person an der Informationserteilung überwiegt oder
- das Bekanntwerden der Informationen die behördliche Strafverfolgung gefährden würde.

[2]Daher erfolgt regelmäßig keine Information über Datenerhebungen zur Aufklärung von Widersprüchlichkeiten gemäß Artikel 15 dieser Verhaltensregeln.

(6) [1]In den Fällen des Absatzes 5 ergreift das Unternehmen geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Personen (z. B. Prüfung und gegebenenfalls Veranlassung weiterer Zugriffsbeschränkungen). [2]Das Unternehmen dokumentiert die Gründe dafür.

Art. 9 Verarbeitung von Stammdaten in der Unternehmensgruppe

(1) [1]Wenn ein Unternehmen (im Sinne der Begriffsbestimmungen dieser Verhaltensregeln, siehe oben zu II.) einer Gruppe von Versicherungs- und Finanzdienstleistungsunternehmen angehört, können die Stammdaten von Antragstellern, Versicherten und weiteren Personen sowie Angaben über den Zusammenhang mit bestehenden Verträgen zur

zentralisierten Bearbeitung von bestimmten Verfahrensabschnitten im Geschäftsablauf (z. B. Telefonate, Post, Inkasso) in einem von gruppenzugehörigen Unternehmen, deren Auftragsverarbeitern und Dienstleistern sowie Vermittlern (im Sinne o. g. Begriffsbestimmungen) gemeinsam nutzbaren Datenverarbeitungsverfahren verarbeitet werden. [2]Dies gilt, wenn sichergestellt ist, dass die technischen und organisatorischen Maßnahmen nach Maßgabe des Artikels 3 dieser Verhaltensregeln (z. B. Berechtigungskonzepte) den datenschutzrechtlichen Anforderungen entsprechen und die Einhaltung dieser Verhaltensregeln durch den oder die für das Verfahren Verantwortlichen gewährleistet ist.

(2) [1]Stammdaten werden aus gemeinsam nutzbaren Datenverarbeitungsverfahren nur weiterverarbeitet, soweit dies für den jeweiligen Zweck erforderlich ist. [2]Dies ist technisch und organisatorisch zu gewährleisten.

(3) [1]Erfolgt eine gemeinsame Verarbeitung von Daten gemäß Absatz 1, treffen die beteiligten Unternehmen die erforderlichen vertraglichen Vereinbarungen nach Artikel 21 bis 22a dieser Verhaltensregeln. [2]Die Versicherten erhalten alle gesetzlich vorgesehenen Informationen und insbesondere die Information über gemeinsame Verarbeitungen nach Absatz 1 bei Vertragsabschluss oder bei Neueinrichtung eines solchen Verfahrens in Textform. [3]Dazu hält das Unternehmen eine aktuelle Liste aller Unternehmen der Gruppe bereit, die an einer zentralisierten Bearbeitung teilnehmen und macht diese in geeigneter Form bekannt. [4]Dabei wird unter Angabe von Kontaktdaten eines primären Ansprechpartners auch darüber informiert, dass betroffene Personen ihre Rechte nach der DSGVO bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen können.

(4) Nimmt ein Unternehmen für ein anderes Mitglied der Gruppe weitere Datenverarbeitungen vor oder finden weitere gemeinsame Verarbeitungen mehrerer Mitglieder der Gruppe statt, richtet sich dies nach Artikel 21 bis 22a dieser Verhaltensregeln.

Art. 10 Statistik, Tarifkalkulation und Prämienberechnung

(1) [1]Die Unternehmen errechnen auf der Basis von Statistiken und Erfahrungswerten mit Hilfe versicherungsmathematischer Methoden die Wahrscheinlichkeit des Eintritts von Versicherungsfällen sowie deren Schadenhöhe und entwickeln auf dieser Grundlage Tarife. [2]Dazu werten Unternehmen neben Daten aus Versicherungsverhältnissen, Leistungs- und Schadenfällen auch andere Daten von Dritten, z. B. des Kraftfahrtbundesamtes (KBA) oder der Fahrzeughersteller, aus.

(2) [1]Die Unternehmen stellen durch geeignete technische und organisatorische Maßnahmen sicher, dass die Rechte und Freiheiten der betroffenen Personen gemäß der DSGVO gewahrt werden und insbesondere die Beachtung des Grundsatzes der Datenminimierung gewährleistet wird, d. h. die Verarbeitung personenbezogener Daten wird auf das für die jeweilige Statistik notwendige Maß beschränkt. [2]Zu diesen Maßnahmen gehört es, die Verarbeitung so durchzuführen, dass die Identifizierung von betroffenen Personen nicht oder möglichst frühzeitig nicht mehr möglich ist, sofern der Statistikzweck auf diese Weise erfüllt werden kann.

(3) [1]Eine Übermittlung von Daten an den Gesamtverband der Deutschen Versicherungswirtschaft e. V., den Verband der Privaten Krankenversicherung e. V. oder andere Stellen zur Errechnung unternehmensübergreifender Statistiken oder Risikoklassifizierungen erfolgt ebenfalls unter Beachtung des Grundsatzes der Datenminimierung im Sinne des Absatzes 2. [2]Die Datensätze werden jedoch unter Verwendung von Kennzeichen

übermittelt, mit denen das übermittelnde Unternehmen Rückfragen zu den Angaben im Datensatz für Zwecke der Qualitätssicherung oder die Treuhänderkontrolle, die teilweise gesetzlich vorgeschrieben ist, zuordnen kann (Identifikationsmerkmale). [3]Dass ein Rückschluss auf die betroffenen Personen durch diese Verbände und Dritte nicht erfolgt, wird durch geeignete technische und organisatorische Maßnahmen bei den Unternehmen, Verbänden und Dritten sichergestellt. [4]Absatz 2 gilt entsprechend.

(4) [1]Für Kraftfahrt- und Sachversicherungsstatistiken können auch Datensätze mit personenbeziehbaren Sachangaben wie z. B. das allgemeine Kfz-Kennzeichen (AKZ), Fahrzeugidentifikationsnummern (FIN) oder Standortdaten von Risikoobjekten wie beispielsweise Gebäuden an den Gesamtverband der Deutschen Versicherungswirtschaft e. V. übermittelt werden. [2]Dies ist insbesondere erforderlich, weil:

- der Verband zur Vervollständigung der Daten aus den Unternehmen für die Kfz-Statistiken Fahrzeugmerkmale vom KBA und von Fahrzeugherstellern (z. B. Angaben über die Art des Aufbaus oder die Ausstattung mit Fahrerassistenzsystemen) mit Hilfe von Abfragen per AKZ oder FIN ergänzt,
- in die Statistik für die Sachversicherung auch die Lage geschädigter Häuser, Lager, Häfen etc. einfließt, um z. B. die Hochwassergefahrenlage oder die Gefahr von Sturmschneisen für das Objekt statistisch berücksichtigen zu können.

(5) [1]Für Datenverarbeitungen zu statistischen Zwecken können Unternehmen auch besondere Kategorien personenbezogener Daten, insbesondere Gesundheitsdaten, verarbeiten, wenn dies für den jeweiligen Statistikzweck erforderlich ist und die Interessen des Verantwortlichen bzw. der Verantwortlichen an der Verarbeitung die Interessen der betroffenen Personen an einem Ausschluss von der Verarbeitung erheblich überwiegen. [2]Das gilt z. B. für Statistiken zur Entwicklung und Überprüfung von Tarifen oder zum gesetzlich vorgeschriebenen Risikomanagement. [3]Die Verantwortlichen treffen in diesen Fällen angemessene und spezifische Maßnahmen gem § 22 Abs. 2 Satz 2 BDSG zur Wahrung der Interessen der betroffenen Personen insbesondere im Sinne der in Artikel 3 dieser Verhaltensregeln geregelten Grundsätze der Datensicherheit. [4]Zu den spezifischen Maßnahmen gehören unter Berücksichtigung der besonderen Schutzbedürftigkeit der Daten beispielsweise:

- die Sensibilisierung der an den Verarbeitungen beteiligten Mitarbeiter und Dienstleister,
- die Verarbeitung personenbezogener Daten so durchzuführen, dass eine Identifikation der betroffenen Person im Sinne von Absatz 2 Satz 2 möglichst frühzeitig ausgeschlossen wird,
- die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der Unternehmen oder beim Dienstleister und
- Verschlüsselung beim Transport personenbezogener Daten.

[5]Alle personenbezogenen Daten werden anonymisiert, sobald dies nach dem Statistikzweck möglich ist, es sei denn, der Anonymisierung stehen berechtigte Interessen der betroffenen Personen entgegen. [6]Bis dahin werden die Identifikationsmerkmale, mit denen Einzelangaben einer betroffenen Person zugeordnet werden könnten, gesondert gespeichert. [7]Diese Identifikationsmerkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Statistikzweck dies erfordert.

(6) [1]Die betroffenen Personen können der Verarbeitung ihrer personenbezogenen Daten für eine Statistik widersprechen, wenn aufgrund ihrer besonderen Situation Gründe vorliegen, die der Verarbeitung ihrer Daten zu diesem Zweck entgegenstehen. [2]Das Widerspruchsrecht besteht nicht, wenn die Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe (z. B. der Beantwortung von Anfragen der Bundesanstalt für Finanzdienstleistungsaufsicht) erforderlich ist.

(7) [1]Zur Ermittlung der risikogerechten Prämie werden Tarife nach Absatz 1 auf die individuelle Situation des Antragstellers angewandt. [2]Darüber hinaus kann eine Bewertung des individuellen Risikos des Antragstellers durch spezialisierte Risikoprüfer, z. B. Ärzte, in die Prämienermittlung einfließen. [3]Hierzu werden auch personenbezogene Daten einschließlich ggf. besonderer Kategorien personenbezogener Daten, wie Gesundheitsdaten, verwendet, die nach Maßgabe dieser Verhaltensregeln verarbeitet worden sind.

(8) [1]Die Unternehmen und Verbände der Versicherungswirtschaft verarbeiten personenbezogene Daten auch für Zwecke der wissenschaftlichen Forschung, zum Beispiel werden:

- für die Unfallforschung des Gesamtverbandes der Deutschen Versicherungswirtschaft e. V. zu den für statistische Zwecke übermittelten Datensätzen schwerer Unfälle von den Unternehmen zusätzlich zu den in Absatz 3 bis 5 genannten Daten weitere Details zum Schaden (z. B. Hergang des Unfalls, Schadenort und -umstände, Alter und Art der Verletzungen von beteiligten Verkehrsteilnehmern) an den Verband übermittelt,
- für Studien des Wissenschaftlichen Instituts der PKV (WIP) im Rahmen der Versorgungsforschung Antrags- und Leistungsdaten der privaten Krankenversicherung übermittelt, beispielsweise zu Verordnungen von Arzneimitteln, Heil- und Hilfsmitteln sowie zur Abrechnung von diagnostischen und therapeutischen Leistungen im Bereich der GOÄ (Gebührenordnung für Ärzte) und GOZ (Gebührenordnung für Zahnärzte).

[2]Die Unternehmen und Verbände können dabei auch mit wissenschaftlichen Forschungseinrichtungen kooperieren.

Art. 11 Scoring

Für das Scoring gelten die gesetzlichen Regelungen.

Art. 12 Bonitätsdaten

Für die Erhebung, Verarbeitung und Nutzung von Bonitätsdaten gelten die gesetzlichen Regelungen.

Art. 13 Automatisierte Einzelentscheidungen

(1) [1]Automatisierte Entscheidungen, die für die betroffenen Personen eine rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen, werden nur dann getroffen, wenn diese datenschutzrechtlich zulässig sind.

(2) [1]Die Unternehmen treffen Entscheidungen automatisiert, wenn diese Art der Entscheidung für den Abschluss oder die Erfüllung eines Versicherungsvertrags mit der betroffenen Person erforderlich ist. [2]Eine Erforderlichkeit automatisierter Entscheidungen kann insbesondere gegeben sein, wenn in folgenden Fällen eine schnelle Entscheidung unerlässlich ist:

1. Entscheidungen gegenüber Antragstellern über den Abschluss und die Konditionen eines Versicherungsvertrages,

2. Entscheidungen über Leistungsfälle im Rahmen eines Versicherungsverhältnisses über Ansprüche von Versicherungsnehmern, versicherten Personen oder Geschädigten.

Dies ist insbesondere in folgenden Fallgruppen möglich:

a) wenn Entscheidungen in sehr großer Menge in kurzer Zeit getroffen werden müssen, z. B. bei massenhaften Schadenfällen nach einem Extremwetter- oder Klimaereignis oder
b) wenn das Unternehmen seine Entscheidungsprozesse aufgrund aufsichtsrechtlicher Vorgaben der Bundesanstalt für Finanzdienstleistungsaufsicht beschleunigen muss oder
c) wenn sich aus der Natur der Entscheidung selbst ergibt, dass diese zeitkritisch ist, wie z. B. bei einer Entscheidung über einen Antrag auf einen innerhalb von Stunden oder wenigen Tagen benötigten Versicherungsschutz, bei einer sofortigen Entscheidung über den Antrag auf Versicherungsschutz im Onlineverfahren bzw. über die Kostenübernahme für einen typischen Bagatellschaden am Kfz oder
d) bei Entscheidungen über die Erfüllung von Merkmalen bei verhaltensbezogenen Tarifen, z. B. das Fahrverhalten honorierende Rabatte in der Kfz-Versicherung.

(3) [1]Automatisierte Entscheidungen über Leistungsansprüche nach einem Versicherungsvertrag, z. B. Entscheidungen gegenüber mitversicherten Personen oder Geschädigten in der Haftpflichtversicherung, sind auch dann zulässig, wenn dem Begehren der betroffenen Person stattgegeben wird. [2]Die Entscheidung kann unabhängig von den Voraussetzungen des Absatzes 2 im Rahmen der Leistungserbringung nach einem Versicherungsvertrag auch automatisiert ergehen, wenn die Entscheidung auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruht und das Unternehmen 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 Unternehmens, auf Darlegung des eigenen Standpunktes und auf Anfechtung der Entscheidung zählt.

(4) Darüber hinaus kann eine automatisierte Entscheidung mit ausdrücklicher Einwilligung der betroffenen Person erfolgen.

(5) [1]Besondere Kategorien personenbezogener Daten werden im Rahmen einer automatisierten Entscheidungsfindung verarbeitet, wenn die betroffenen Personen ihre Einwilligung erteilt haben. [2]Automatisierte Entscheidungen mit besonderen Kategorien personenbezogener Daten sind auch ohne Einwilligung in den Fällen des Absatzes 3 möglich.

(6) Der Einsatz automatisierter Entscheidungsverfahren wird dokumentiert.

(7) [1]Die Unternehmen stellen sicher, dass technische und organisatorische Maßnahmen getroffen werden, damit Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden können und das Risiko von Fehlern minimiert wird.

Art. 14 Hinweis- und Informationssystem (HIS)

(1) [1]Unternehmen der deutschen Versicherungswirtschaft nutzen ein Hinweis- und Informationssystem (HIS) zur Unterstützung der Risikobeurteilung im Antragsfall, zur Sachverhaltsaufklärung bei der Leistungsprüfung sowie bei der Bekämpfung der missbräuchlichen Erlangung von Versicherungsleistungen. [2]Der Betrieb und die Nutzung des HIS erfolgen auf Basis von Interessenabwägungen und festgelegten Einmeldekriterien.

(2) [1]Das HIS wird getrennt nach Versicherungssparten betrieben. [2]In allen Sparten wird der Datenbestand in jeweils zwei Datenpools getrennt verarbeitet: in einem Datenpool für die Abfrage zur Risikoprüfung im Antragsfall (A-Pool) und in einem Pool für die Abfrage zur Leistungsprüfung (L-Pool). [3]Die Unternehmen richten die Zugriffsberechtigungen für ihre Mitarbeiter entsprechend nach Sparten und Aufgaben getrennt ein.

(3) [1]Die Unternehmen melden Daten zu Fahrzeugen, Immobilien oder Personen an den Betreiber des HIS, wenn ein erhöhtes Risiko vorliegt oder wenn eine Auffälligkeit festgestellt wurde, soweit dies zur gegenwärtigen oder künftigen Aufdeckung oder zur Verhinderung der missbräuchlichen Erlangung von Versicherungsleistungen erforderlich ist und nicht überwiegende schutzwürdige Rechte und Freiheiten der betroffenen Personen dagegen sprechen. [2]Eine Einwilligung der betroffenen Personen ist nicht erforderlich. [3]Vor einer Einmeldung von Daten zu Personen erfolgt eine Abwägung der Interessen der Unternehmen und des Betroffenen. [4]Bei Vorliegen der festgelegten Meldekriterien ist regelmäßig von einem überwiegenden berechtigten Interesse des Unternehmens an der Einmeldung auszugehen. [5]Die Abwägung ist zu dokumentieren. [6]Besondere Kategorien personenbezogener Daten, wie z. B. Gesundheitsdaten, werden nicht an das HIS gemeldet. [7]Wenn erhöhte Risiken in der Personenversicherung als „Erschwernis“ gemeldet werden, geschieht dies ohne die Angabe, ob sie auf Gesundheitsdaten oder einem anderen Grund, z. B. einem gefährlichen Beruf oder Hobby, beruhen.

(4) [1]Die Unternehmen informieren die Versicherungsnehmer bereits bei Vertragsabschluss in allgemeiner Form über das HIS unter Angabe des Verantwortlichen mit dessen Kontaktdaten. [2]Sie benachrichtigen spätestens anlässlich der Einmeldung die betroffenen Personen mit den in Artikel 8 Abs. 3 genannten Informationen. [3]Eine Benachrichtigung kann in den Fällen des Artikel 8 Abs. 5 dieser Verhaltensregelungen unterbleiben.

(5) [1]Ein Abruf von Daten aus dem HIS kann bei Antragstellung und im Leistungsfall erfolgen, nicht jedoch bei Auszahlung einer Kapitallebensversicherung im Erlebensfall. [2]Der Datenabruf ist nicht die alleinige Grundlage für eine Entscheidung im Einzelfall. [3]Die Informationen werden lediglich als Hinweis dafür gewertet, dass der Sachverhalt einer näheren Prüfung bedarf. [4]Alle Datenabrufe erfolgen im automatisierten Abrufverfahren und werden protokolliert für Revisionszwecke und den Zweck, stichprobenartig deren Berechtigung prüfen zu können.

(6) [1]Soweit zur weiteren Sachverhaltsaufklärung erforderlich, können im Leistungsfall auch Daten zwischen dem einmeldenden und dem abrufenden Unternehmen ausgetauscht werden, wenn kein Grund zu der Annahme besteht, dass die betroffene Person ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. [2]So werden beispielsweise Daten und Gutachten über Kfz- oder Gebäude-Schäden bei dem Unternehmen angefordert, welches einen Schaden in das HIS eingemeldet hatte. [3]Der Datenaustausch wird dokumentiert. [4]Soweit der Datenaustausch nicht gemäß Artikel 15 dieser Verhaltensregeln erfolgt, werden die betroffenen Personen über den Datenaustausch

informiert. [5]Eine Information ist nicht erforderlich, solange die Aufklärung des Sachverhalts dadurch gefährdet würde oder wenn die betroffenen Personen auf andere Weise Kenntnis vom Datenaustausch erlangt haben.

(7) [1]Die im HIS gespeicherten Daten werden spätestens am Ende des 4. Jahres nach dem Vorliegen der Voraussetzung für die Einmeldung gelöscht. [2]Zu einer Verlängerung der Speicherdauer auf maximal 10 Jahre kommt es in der Lebensversicherung im Leistungsbereich oder bei erneuter Einmeldung innerhalb der regulären Speicherzeit gemäß Satz 1. [3]Daten zu Anträgen, bei denen kein Vertrag zustande gekommen ist, werden im HIS spätestens am Ende des 3. Jahres nach dem Jahr der Antragstellung gelöscht.

(8) Der Gesamtverband der Deutschen Versicherungswirtschaft e. V. gibt unter Beachtung datenschutzrechtlicher Vorgaben einen detaillierten Leitfaden zur Nutzung des HIS an die Unternehmen heraus.

Art. 15 Aufklärung von Widersprüchlichkeiten

(1) [1]Die Unternehmen können jederzeit bei entsprechenden Anhaltspunkten für Widersprüchlichkeiten prüfen, ob bei der Antragstellung oder bei Aktualisierungen von Antragsdaten während des Versicherungsverhältnisses unrichtige oder unvollständige Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde oder ob falsche oder unvollständige Sachverhaltsangaben bei der Feststellung eines entstandenen Schadens gemacht wurden. [2]Zu diesem Zweck nehmen die Unternehmen Datenerhebungen und -verarbeitungen vor, soweit dies zur Aufklärung der Widersprüchlichkeiten erforderlich ist. [3]Bei der Entscheidung, welche Daten die Unternehmen benötigen, um ihre Entscheidung auf ausreichender Tatsachenbasis zu treffen, kommt ihnen ein Beurteilungsspielraum zu.

(2) [1]Anhaltspunkte für Widersprüchlichkeiten im Sinne des Abs.1 liegen vor, wenn nach Aktenlage zum Zeitpunkt der Datenverarbeitung Anhaltspunkte dafür bestehen, dass vorsätzlich oder fahrlässig unrichtige Angaben gemacht wurden, die für die Risiko- oder Leistungsprüfung relevant sind. [2]Dies ist beispielsweise der Fall, wenn Angaben zum Schadenhergang nicht zum Schadenbild passen oder wenn geltend gemachte Schäden erkennbar älter sein müssen als das als Ursache benannte Schadenereignis.

(3) [1]Im Leistungsfall kann auch ohne Vorliegen von Anhaltspunkten die Prüfung nach Abs. 1 erfolgen. [2]Dies umfasst die Einholung von Vorinformationen (z. B. Zeiträume, in denen Behandlungen oder Untersuchungen stattfanden), die es dem Unternehmen ermöglichen einzuschätzen, ob und welche Informationen im Weiteren tatsächlich für die Prüfung relevant sind.

(4) [1]Datenverarbeitungen zur Überprüfung der Angaben zur Risikobeurteilung bei Antragstellung erfolgen gemäß § 21 Abs. 3 Satz 1 VVG regelmäßig nur innerhalb von fünf Jahren, bei Krankenversicherungen gemäß § 194 Abs. 1 Satz 4 VVG innerhalb von drei Jahren nach Vertragsschluss. [2]Die Angaben können auch nach Ablauf dieser Zeit noch überprüft werden, wenn der Versicherungsfall vor Ablauf der Frist eingetreten ist. [3]Für die Prüfung, ob der Versicherungsnehmer bei der Antragstellung vorsätzlich oder arglistig unrichtige oder unvollständige Angaben gemacht hat, verlängert sich dieser Zeitraum gemäß § 21 Abs. 3 Satz 2 VVG auf 10 Jahre.

(5) Ist die Erhebung und Verarbeitung von besonderen Kategorien personenbezogener Daten, insbesondere von Daten über die Gesundheit, nach Absatz 1 bis 3 erforderlich, werden die betroffenen Personen entsprechend ihrer Erklärung im Versicherungsantrag vor einer Datenerhebung bei Dritten nach § 213 Abs. 2 VVG unterrichtet und auf ihr Widerspruchsrecht hingewiesen oder von den betroffenen Personen wird zuvor eine eigenständige Einwilligungs- und Schweigepflichtentbindungserklärung eingeholt.

(6) [1]Die Möglichkeit, die Abgabe der Einwilligungs- und Schweigepflichtentbindungserklärung zu verweigern, bleibt unbenommen und das Unternehmen informiert die betroffene Person diesbezüglich. [2]Verweigert die betroffene Person die Abgabe der Einwilligungs- und Schweigepflichtentbindungserklärung, obliegt es der betroffenen Person als Voraussetzung für die Schadenregulierung, alle erforderlichen Informationen zu beschaffen und dem Unternehmen zur Verfügung zu stellen. [3]Das Unternehmen hat in diesem Fall darzulegen, welche Informationen es bei Verweigerung der Einwilligungs- und Schweigepflichtentbindungserklärung für erforderlich hält.

Art. 16 Datenaustausch mit anderen Versicherern

(1) [1]Ein Datenaustausch zwischen einem Vorversicherer und seinem nachfolgenden Versicherer wird zur Erhebung tarifrelevanter oder leistungsrelevanter Angaben unter Beachtung des Artikels 8 dieser Verhaltensregeln vorgenommen. [2]Dies ist insbesondere der Fall, wenn die Angaben erforderlich sind:

1. bei der Risikoeinschätzung zur Überprüfung von Schadenfreiheitsrabatten, insbesondere der Schadensfreiheitsklassen in der Kfz-Haftpflichtversicherung und Vollkaskoversicherung,

2. zur Übertragung von Ansprüchen auf Altersvorsorge bei Anbieter- oder Arbeitgeberwechsel,

3. zur Übertragung von Altersrückstellungen in der Krankenversicherung auf den neuen Versicherer,

4. zur Ergänzung oder Verifizierung der Angaben der Antragsteller oder Versicherten.

[3]In den Fällen der Nummern 1 und 4 ist der Datenaustausch zum Zweck der Risikoprüfung nur zulässig, wenn die betroffenen Personen bei Datenerhebung im Antrag über den möglichen Datenaustausch und dessen Zweck und Gegenstand informiert werden. [4]Nach einem Datenaustausch zum Zweck der Leistungsprüfung werden die betroffenen Personen vom Daten erhebenden Unternehmen über einen erfolgten Datenaustausch im gleichen Umfang informiert. [5]Artikel 15 dieser Verhaltensregeln bleibt unberührt.

(2) Ein Datenaustausch mit anderen Versicherern außerhalb der für das Hinweis- und Informationssystem der Versicherungswirtschaft (HIS) getroffenen Regelungen erfolgt darüber hinaus, soweit dies zur Antrags- und Leistungsprüfung und -erbringung, einschließlich der Regulierung von Schäden bei gemeinsamer, mehrfacher oder kombinierter Absicherung von Risiken, des gesetzlichen Übergangs einer Forderung gegen eine andere Person oder zur Regulierung von Schäden zwischen mehreren Versicherern über bestehende Teilungs- und Regressverzichtsabkommen erforderlich ist und kein Grund zu der Annahme besteht, dass ein überwiegendes schutzwürdiges Interesse der betroffenen Person dem entgegensteht.

(3) Der Datenaustausch wird dokumentiert.

Art. 17 Datenübermittlung an Rückversicherer

(1) [1]Um jederzeit zur Erfüllung ihrer Verpflichtungen aus den Versicherungsverhältnissen in der Lage zu sein, geben Unternehmen einen Teil ihrer Risiken aus den Versicherungsverträgen an Rückversicherer weiter. [2]Zum weiteren Risikoausgleich bedienen sich in einigen Fällen diese Rückversicherer ihrerseits weiterer Rückversicherer. [3]Zur ordnungsgemäßen Begründung, Durchführung oder Beendigung des Rückversicherungsvertrages werden Daten aus dem Versicherungsantrag oder -verhältnis in anonymisierter Form oder – soweit dies für die vorgenannten Zwecke nicht ausreichend ist – so verarbeitet, dass die Identifizierung von betroffenen Personen nicht oder möglichst frühzeitig nicht mehr möglich ist, insbesondere können Versicherungsnummer, Beitrag, Art und Höhe des Versicherungsschutzes und des Risikos sowie etwaige Risikozuschläge weitergegeben werden.

(2) [1]Personenbezogene Daten erhalten die Rückversicherer nur, soweit dies

1. für den Abschluss oder die Erfüllung des Versicherungsvertrages erforderlich ist oder
2. zur Sicherstellung der Erfüllbarkeit der Verpflichtungen des Unternehmens aus den Versicherungsverhältnissen erfolgt und kein Grund zu der Annahme besteht, dass ein überwiegendes schutzwürdiges Interesse der betroffenen Person dem Unternehmensinteresse entgegensteht.

[2]Dies kann der Fall sein, wenn im Rahmen des konkreten Rückversicherungsverhältnisses die Übermittlung personenbezogener Daten an Rückversicherer aus folgenden Gründen erfolgt:

a) Die Rückversicherer führen z. B. bei hohen Vertragssummen oder bei einem schwer einzustufenden Risiko im Einzelfall die Risikoprüfung und die Leistungsprüfung durch.
b) Die Rückversicherer unterstützen die Unternehmen bei der Risiko- und Schadenbeurteilung sowie bei der Bewertung von Verfahrensabläufen.
c) Die Rückversicherer erhalten zur Bestimmung des Umfangs der Rückversicherungsverträge einschließlich der Prüfung, ob und in welcher Höhe sie an ein und demselben Risiko beteiligt sind (Kumulkontrolle) sowie zu Abrechnungszwecken Listen über den Bestand der unter die Rückversicherung fallenden Verträge.
d) Die Risiko- und Leistungsprüfung durch den Erstversicherer wird von den Rückversicherern stichprobenartig oder in Einzelfällen kontrolliert zur Prüfung ihrer Leistungspflicht gegenüber dem Erstversicherer.

(3) [1]Die Unternehmen vereinbaren mit den Rückversicherern, dass personenbezogene Daten von diesen nur zu den in Absatz 2 genannten Zwecken sowie mit diesen kompatiblen Zwecken (z. B. Statistiken und wissenschaftliche Forschung unter Beachtung des Art. 89 DSGVO, Risiko- und Produktmanagement, einschließlich deren Weiterentwicklung, Erfüllung aufsichtsrechtlicher Vorgaben) verwendet werden. [2]So nutzen Rückversicherer die von den Unternehmen erhaltenen Daten insbesondere auch zu statistischen Zwecken, um Risiken besser einschätzen zu können und ihre Prämien entsprechend den aufsichtsrechtlichen Vorgaben zu berechnen. [3]Dafür werden beispielsweise Daten der

Schäden aus Naturkatastrophen ausgewertet, um die Bewertung und Prognose von Risiken des Klimawandels zu beurteilen und zu optimieren. [4]Zu wissenschaftlichen Forschungszwecken können die Daten verarbeitet werden, um neu auftretende oder sich verändernde Risiken erkennen und deren Versicherbarkeit einschätzen zu können, beispielsweise die Auswirkungen extremer Hitze oder des erhöhten Konsums hochverarbeiteter Lebensmittel, die Ausbreitung von Pilzkrankheiten oder die Gefahren durch Kunststoffe in der Umwelt. [5]In der medizinischen Forschung der Rückversicherer werden die Chancen und Risiken neuer Diagnose- und Behandlungsmöglichkeiten von Erkrankungen untersucht, um wissenschaftliche Grundlagen für eine zeitgemäße, risikogerechte, diskriminierungsfreie Versicherbarkeit im Sinne der Branche und der betroffenen Personen zu schaffen.

(4) [1]Die Unternehmen vereinbaren mit den Rückversicherern außerdem, ob der Rückversicherer eine gesetzlich erforderliche Information an die betroffene Person selbst vornimmt oder ob das Unternehmen die Information des Rückversicherers an die betroffene Person weiterleitet. [2]Im Fall der Weiterleitung vereinbaren sie auch, wie die Information erfolgt. [3]Soweit die Unternehmen einer Verschwiegenheitspflicht gemäß § 203 StGB unterliegen, verpflichten sie die Rückversicherer hinsichtlich der Daten, die sie nach Absatz 2 erhalten, Verschwiegenheit zu wahren und weitere Rückversicherer sowie Stellen, die für sie tätig sind, zur Verschwiegenheit zu verpflichten.

(5) Besondere Kategorien personenbezogener Daten, insbesondere Gesundheitsdaten, erhalten die Rückversicherer nur, wenn die Voraussetzungen des Artikels 6 dieser Verhaltensregeln erfüllt sind.

V. VERARBEITUNG PERSONENBEZOGENER DATEN FÜR VERTRIEBSZWECKE UND ZUR MARKT- UND MEINUNGSFORSCHUNG

Art. 18 Verwendung von Daten für Zwecke der Werbung

(1) [1]Personenbezogene Daten dürfen für Werbezwecke nur auf Grundlage von Art. 6 Abs. 1 lit. a) oder f) DSGVO verarbeitet werden. [2]Dabei sind § 7 und § 7a UWG zu beachten.

(2) [1]Betroffene Personen können der Verwendung ihrer personenbezogenen Daten für Zwecke der Direktwerbung widersprechen. [2]In diesem Fall werden die personenbezogenen Daten nicht mehr zu diesen Zwecken verarbeitet. [3]Das Unternehmen trifft zur Umsetzung geeignete technische und organisatorische Maßnahmen.

Art. 19 Marktumfragen

(1) [1]Die Unternehmen führen Markt- und Meinungsumfragen mit Einwilligung der betroffenen Personen gem. Art. 6 Abs. 1 lit. a) DSGVO oder nach Interessenabwägung gemäß Art. 6 Abs. 1 f) DSGVO durch. [2]Die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke der Markt- und Meinungsforschung erfolgt nur mit Einwilligung der betroffenen Personen oder gem. Art. 6 Abs. 1 lit. f) DSGVO, wenn diese ihre Daten offensichtlich selbst öffentlich gemacht haben.

(2) [1]Soweit die Unternehmen andere Stellen mit Markt- und Meinungsumfragen beauftragen, sind die Einzelheiten des Vorhabens vertraglich nach den Vorgaben der Artikel 21, 22 oder 22a dieser Verhaltensregeln zu regeln. [2]Dabei ist insbesondere festzulegen:

a) dass die übermittelten und zusätzlich erhobenen Daten so verarbeitet werden, dass eine Identifikation der betroffenen Person frühestmöglich ausgeschlossen wird,
b) dass die Auswertung der Daten in möglichst anonymisierter Form oder unter einem der Zuordnung des Teilnehmers dienenden Kennzeichen erfolgt, wenn dies für die Zwecke erforderlich ist (z. B. Folgebefragungen),
c) dass die Markt- und Meinungsforschung auf einem wissenschaftlich-methodischen Vorgehen beruhen muss,
d) dass die Daten ausschließlich für die Zwecke der jeweils beauftragten Markt- und Meinungsforschung verwendet werden dürfen sowie
e) dass die Übermittlung der Ergebnisse der Markt- und Meinungsumfragen an die Unternehmen nur in anonymisierter Form erfolgt.

(3) Soweit die Unternehmen selbst personenbezogene Daten zum Zweck der Durchführung von Markt- und Meinungsumfragen verarbeiten oder nutzen, gelten die in Absatz 2 lit. a) bis e) festgelegten Vorgaben ebenfalls.

(4) [1]Zur Marktforschung gewonnene personenbezogene Daten dürfen nicht zu Werbe- und Marketingzwecken verwendet werden. [2]Soweit im Rahmen der Markt- und Meinungsumfragen geschäftliche Handlungen vorgenommen werden, die als Werbung zu werten sind, beispielsweise wenn bei der Datenerhebung auch absatzfördernde Äußerungen erfolgen, richtet sich die Verarbeitung personenbezogener Daten dafür nach den in Artikel 18 dieser Verhaltensregeln getroffenen Regelungen. [3]Bei einer beabsichtigten werblichen Nutzung der Daten ist hierfür eine vorherige informierte Einwilligung von den Betroffenen einzuholen.

Art. 20 Datenübermittlung an selbstständige Vermittler

(1) [1]Eine Übermittlung personenbezogener Daten erfolgt an den betreuenden Vermittler nur, soweit es zur bedarfsgerechten Vorbereitung oder Bearbeitung eines konkreten Antrags bzw. Vertrags oder zur ordnungsgemäßen Durchführung der Versicherungsangelegenheiten der betroffenen Personen erforderlich ist. [2]Die Vermittler werden auf ihre besonderen Verschwiegenheitspflichten hingewiesen.

(2) [1]Vor der erstmaligen Übermittlung personenbezogener Daten an einen Versicherungsvertreter oder im Falle eines Wechsels vom betreuenden Versicherungsvertreter auf einen anderen Versicherungsvertreter informiert das Unternehmen die Versicherten oder Antragsteller vorbehaltlich der Regelung des Absatz 3 möglichst frühzeitig, mindestens aber zwei Wochen vor der Übermittlung ihrer personenbezogenen Daten über den bevorstehenden Datentransfer, die Identität (Name, Sitz) des neuen Versicherungsvertreters und ihr Widerspruchsrecht. [2]Die Benachrichtigung erfolgt nicht, wenn der Wechsel von der betroffenen Person selbst gewünscht ist. [3]Eine Information durch den bisherigen Versicherungsvertreter steht einer Information durch das Unternehmen gleich. [4]Im Falle eines Widerspruchs findet die Datenübermittlung grundsätzlich nicht statt. [5]In diesem Fall wird die Betreuung durch einen anderen Versicherungsvertreter oder das Unternehmen selbst angeboten.

(3) Eine Ausnahme von der in Absatz 2 Satz 1 geregelten 2-Wochenfrist besteht, wenn die ordnungsgemäße Betreuung der Versicherten im Einzelfall oder wegen des unerwarteten Wegfalls der Betreuung des Bestandes der Vertragsverhältnisse gefährdet ist.

(4) [1]Personenbezogene Daten von Versicherten oder Antragstellern dürfen an einen Versicherungsmakler oder eine Dienstleistungsgesellschaft von Versicherungsmaklern übermittelt werden, wenn die Versicherten oder Antragsteller dem Makler dafür eine Maklervollmacht oder eine vergleichbare Bevollmächtigung erteilt haben, die die Datenübermittlung abdeckt. [2]Für den Fall des Wechsels des Maklers gilt zudem Absatz 2 entsprechend.

(5) [1]Eine Übermittlung von Gesundheitsdaten durch das Unternehmen an den betreuenden Vermittler erfolgt grundsätzlich nicht, es sei denn, es liegt eine Einwilligung der betroffenen Personen vor. [2]Gesetzliche Übermittlungsbefugnisse bleiben hiervon unberührt.

VI. DATENVERARBEITUNG DURCH AUFTRAGSVERARBEITER, DIENSTLEISTER UND GEMEINSAM VERANTWORTLICHE

Art. 21 Pflichten bei der Verarbeitung im Auftrag

(1) Sofern ein Unternehmen personenbezogene Daten im Auftrag verarbeiten lässt (z. B. können folgende Aufgaben ganz oder teilweise an weisungsgebundene Auftragsverarbeiter übertragen werden: elektronische Datenverarbeitung, Scannen und Zuordnung von Eingangspost, Adressverwaltung, Antrags- und Vertragsbearbeitung, Schaden- und Leistungsbearbeitung, Sicherstellung der korrekten Verbuchung von Zahlungseingängen, Zahlungsausgang, Entsorgung von Dokumenten), kommt Art. 28 DSGVO zur Anwendung.

(2) Vertragsklauseln sollen den Datenschutzbeauftragten vorgelegt werden, die bei Bedarf beratend mitwirken.

(3) [1]Das Unternehmen hält eine aktuelle Liste der Auftragnehmer bereit. [2]Auftragnehmer können unter Bezeichnung ihrer Aufgaben – unbeschadet interner Dokumentationspflichten – in Kategorien zusammengefasst werden, wenn:

- die Verarbeitung personenbezogener Daten nicht zur Erfüllung versicherungsspezifischer Aufgaben und Zwecke dient oder
- der Rechercheaufwand zu groß ist oder
- überwiegende berechtigte Interessen, wie beispielsweise Geheimhaltungsinteressen, bestehen oder
- viele verschiedene Auftragnehmer (z. B. Dienstleister zur Aktenvernichtung an verschiedenen Unternehmensstandorten oder regionale Werkstätten) mit gleichartigen Aufgaben betraut werden oder
- Auftragnehmer nur gelegentlich tätig werden.

[3]Die Liste wird in geeigneter Form bekannt gegeben. [4]Werden personenbezogene Daten bei den betroffenen Personen erhoben, sind diese grundsätzlich bei Erhebung über die Liste zu unterrichten.

Art. 22 Datenverarbeitung durch eigenverantwortliche Dienstleister

(1) [1]Ohne Vereinbarung einer Auftragsverarbeitung können personenbezogene Daten an Dienstleister zur eigenverantwortlichen Aufgabenerfüllung übermittelt und von diesen verarbeitet werden, soweit dies für die Zweckbestimmung des Versicherungsverhältnisses mit den betroffenen Personen erforderlich ist. [2]Das ist insbesondere möglich, wenn

Sachverständige mit der Begutachtung eines Versicherungsfalls beauftragt sind oder wenn Dienstleister zur Ausführung der vertraglich vereinbarten Versicherungsleistungen, die eine Sachleistung beinhalten, eingeschaltet werden, z. B. Krankentransportdienstleister, Haushaltshilfen, Schlüsseldienste und ähnliche Dienstleister.

(2) [1]Die Verarbeitung von personenbezogenen Daten zur eigenverantwortlichen Erfüllung von Datenverarbeitungs- oder sonstigen Aufgaben beim Dienstleister kann auch dann erfolgen, wenn dies zur Wahrung der berechtigten Interessen des Unternehmens erforderlich ist und die schutzwürdigen Interessen der betroffenen Personen nicht überwiegen. [2]Das kann zum Beispiel der Fall sein, wenn Dienstleister Aufgaben übernehmen, die der Geschäftsabwicklung des Unternehmens dienen, wie beispielsweise die Risikoprüfung, Schaden- und Leistungsbearbeitung und Inkasso, sofern dies keine Auftragsverarbeitung ist und die Voraussetzungen der Absätze 4 bis 8 erfüllt sind.

(3) In allen in den Absätzen 1 und 2 genannten Fällen ist der Dienstleister Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

(4) [1]Die Übermittlung von personenbezogenen Daten an Dienstleister nach Absatz 2 unterbleibt, soweit die betroffene Person aus Gründen, die sich aus ihrer besonderen persönlichen Situation ergeben, dieser widerspricht und eine Prüfung ergibt, dass seitens des übermittelnden Unternehmens keine zwingenden schutzwürdigen Gründe für die Verarbeitung beim Dienstleister vorliegen, die die Interessen der betroffenen Person überwiegen. [2]Die Übermittlung an den Dienstleister erfolgt trotz des Widerspruchs auch dann, wenn sie der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient. [3]Die betroffenen Personen werden in geeigneter Weise auf ihre Widerspruchsmöglichkeit hingewiesen.

(5) Das Unternehmen schließt mit den Dienstleistern, die nach Absatz 2 tätig werden, eine vertragliche Vereinbarung, die mindestens folgende Punkte enthalten muss:

a) Eindeutige Beschreibung der Aufgaben des Dienstleisters;
b) Sicherstellung, dass die übermittelten Daten nur im Rahmen der vereinbarten Zweckbestimmung verarbeitet oder genutzt werden;
c) Gewährleistung eines Datenschutz- und Datensicherheitsstandards, der diesen Verhaltensregeln entspricht;
d) Verpflichtung des Dienstleisters, dem Unternehmen alle Auskünfte zu erteilen, die zur Erfüllung einer beim Unternehmen verbleibenden Auskunftspflicht erforderlich sind oder der betroffenen Person direkt Auskunft zu erteilen.

(6) Diese Aufgabenauslagerungen nach Absatz 2 werden dokumentiert.

(7) Unternehmen und Dienstleister haften in den Fällen des Absatzes 2 als an der Verarbeitung der Daten für die jeweiligen Zwecke und Aufgaben beteiligte Verantwortliche gemäß Art. 82 DSGVO; insbesondere sind das Unternehmen und der Dienstleister verantwortlich für Datenverarbeitungen gemäß der Absätze 2 bis 5 dieser Vorschrift.

(8) [1]Das Unternehmen hält eine aktuelle Liste der Dienstleister nach Absatz 2 bereit. [2]Die Dienstleister können unter den in Artikel 21 Abs. 3 genannten Voraussetzungen unter Bezeichnung ihrer Aufgaben in Kategorien zusammengefasst werden. [3]Die Liste wird in geeigneter Form bekannt gegeben. [4]Werden personenbezogene Daten bei den Betroffenen erhoben, sind sie grundsätzlich bei Erhebung über die Liste zu unterrichten.

(9) Übermittlungen von personenbezogenen Daten an Rechtsanwälte, Steuerberater und Wirtschaftsprüfer im Rahmen von deren Aufgabenerfüllungen bleiben von den zuvor genannten Regelungen unberührt.

(10) [1]Besondere Kategorien personenbezogener Daten dürfen in diesem Rahmen nur verarbeitet werden, wenn die betroffenen Personen eingewilligt haben oder eine sonstige Ausnahme nach Art. 9 Abs. 2 DSGVO und eine gesetzliche Grundlage vorliegt. [2]Soweit die Unternehmen einer Verschwiegenheitspflicht gemäß § 203 StGB unterliegen, verpflichten sie die Dienstleister hinsichtlich der Daten, die sie nach den Absätzen 1 und 2 erhalten, Verschwiegenheit zu wahren und weitere Dienstleister sowie Stellen, die für sie tätig sind, zur Verschwiegenheit zu verpflichten.

Art. 22a Gemeinsam verantwortliche Stellen

(1) Eine Gruppe von Versicherungs- und Finanzdienstleistungsunternehmen kann für gemeinsame Geschäftszwecke gemeinsame Datenverarbeitungsverfahren nach Maßgabe des Art. 26 DSGVO einrichten.

(2) [1]Das Unternehmen hält eine aktuelle Liste der Zwecke der gemeinsamen Datenverarbeitungsverfahren mit den jeweils verantwortlichen Unternehmen bereit und gibt sie den betroffenen Personen in geeigneter Form bekannt. [2]Dabei wird ggf. unter Angabe von Kontaktdaten eines primären Ansprechpartners auch darüber informiert, dass betroffene Personen ihre Rechte nach der DSGVO bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen können (vgl. Artikel 9 Abs. 3 Satz 4).

VII. RECHTE DER BETROFFENEN PERSONEN

Art. 23 Auskunftsanspruch

(1) [1]Betroffene Personen haben das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. [2]Ist dies der Fall, so haben sie ein Recht auf Auskunft über die beim Unternehmen über sie verarbeiteten Daten und die in Art. 15 DSGVO genannten Informationen.

(2) [1]Verarbeitet ein Unternehmen eine große Menge von Informationen über die betroffene Person oder wird ein Auskunftsersuchen im Hinblick auf die zu beauskunftenden personenbezogenen Daten unspezifisch gestellt, erteilt das Unternehmen in einer ersten Stufe zunächst Auskunft über die zur betroffenen Person gespeicherten Stammdaten sowie zusammenfassende Informationen nach Art. 15 Abs. 1 und 2 DSGVO über die Verarbeitung ihrer Daten für Antrags- oder Vertragsbeziehungen zum Unternehmen. [2]Das Unternehmen bittet die betroffene Person auf dieser Stufe zu präzisieren, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Verlangen bezieht. [3]Dafür erteilt das Unternehmen der betroffenen Person aussagekräftige Informationen über die Verarbeitungsvorgänge, die für die betroffene Person von Belang sein könnten, und weist ergänzend darauf hin, dass zum Beispiel durch Benennung eines Zeitraumes und eines konkreten Geschäftsvorgangs die Möglichkeit besteht, gezielt nach weitergehenden Daten zu suchen und diese zu beauskunften. [4]Bestätigt die betroffene Person, die gebeten wurde, den Umfang ihres Auskunftsantrags zu präzisieren, dass sie alle sie betreffenden personenbezogenen Daten anfordert, stellt das Unternehmen der betroffenen Person alle gesetzlich vorgesehenen Informationen zur Verfügung.

(3) [1]Es wird sichergestellt, dass nur die berechtigte Person die Auskunft erhält. [2]Daher wird Bevollmächtigten die Auskunft nur erteilt, wenn die Empfangsbevollmächtigung ausreichend nachgewiesen ist.

(4) [1]Eine Auskunft erfolgt schriftlich oder in anderer Form, insbesondere auch elektronisch, beispielsweise in einem Kundenportal. [2]Im Falle einer elektronischen Antragstellung werden die Informationen in einem gängigen elektronischen Format zur Verfügung gestellt. [3]Dies erfolgt nicht, wenn etwas anderes gewünscht ist oder die sichere Übermittlung auf elektronischem Weg nicht gewährleistet werden kann. [4]Sie kann auf Verlangen der betroffenen Personen auch mündlich erfolgen, aber nur sofern die Identität der betroffenen Personen nachgewiesen wurde.

(5) [1]Durch die Auskunft dürfen nicht die Rechte und Freiheiten weiterer Personen beeinträchtigt werden. [2]Geschäftsgeheimnisse des Unternehmens können berücksichtigt werden.

(6) [1]Eine Auskunft kann unterbleiben, wenn die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen des überwiegenden berechtigten Interesses eines Dritten, geheim gehalten werden müssen oder wenn das Bekanntwerden der Information die Strafverfolgung gefährden würde. [2]Eine Auskunft unterbleibt ferner über Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder sie ausschließlich Zwecken der Datensicherung oder Datenschutzkontrolle dienen, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist; Beispiele können wegen Aufbewahrungspflichten in der Verarbeitung eingeschränkte Daten und zugriffsgeschützte Sicherungskopien (Backups) sein.

(7) [1]In Fällen des Absatzes 6 werden die Gründe der Auskunftsverweigerung dokumentiert. [2]Die Ablehnung der Auskunftserteilung wird gegenüber der betroffenen Person begründet. [3]Die Begründung erfolgt nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde, insbesondere wenn die Mitteilung der Gründe die überwiegenden berechtigten Interessen Dritter oder die Strafverfolgung beeinträchtigen würde.

(8) Im Falle einer Rückversicherung (Artikel 17), Datenverarbeitung durch eigenverantwortliche Dienstleister (Artikel 22) oder Verarbeitung durch gemeinsam Verantwortliche (Artikel 22a) nimmt das Unternehmen die Auskunftsverlangen entgegen und erteilt auch alle Auskünfte, zu denen der Rückversicherer, Dienstleister oder alle Verantwortlichen verpflichtet sind oder es stellt die Auskunftserteilung durch diese sicher.

Art. 24 Recht auf Datenübertragbarkeit

[1]Das Recht auf Datenübertragbarkeit nach Art. 20 DSGVO umfasst die Daten, die die betroffene Person gegenüber dem Unternehmen angegeben oder bereitgestellt hat. [2]Das sind beispielsweise die Daten, die von der betroffenen Person in Anträgen angegeben wurden, wie Name, Adresse und die zum zu versichernden Risiko erfragten Angaben sowie alle weiteren im Laufe des Versicherungsverhältnisses gemachten personenbezogenen Angaben, zum Beispiel bei Schadenmeldungen bereitgestellte Daten.

Art. 25 Löschung

(1) [1]Die Prüfung des Datenbestandes auf die Notwendigkeit einer Löschung nach Art. 5 Abs. 1 lit. e) und Art. 17 Abs 1 DSGVO erfolgt in regelmäßigen Abständen, mindestens einmal jährlich. [2]Auf Verlangen der betroffenen Person wird unverzüglich geprüft, ob die von dem Verlangen erfassten Daten zu löschen sind.

(2) [1]Eine Löschung nach Absatz 1 erfolgt gem. Art. 17 Abs. 3 DSGVO insbesondere nicht, soweit die Daten erforderlich sind:

a) zur Erfüllung einer rechtlichen Verpflichtung des Unternehmens, insbesondere zur Erfüllung gesetzlicher Aufbewahrungspflichten,
b) für die in Artikel 10 genannten Verarbeitungen für statistische Zwecke gemäß Art. 89 Abs. 1 DSGVO,
c) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke (z. B. zur Aufarbeitung des Holocaust) gemäß Art. 89 Abs.1 DSGVO oder
d) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

[2]Ein Verzicht auf die Löschung ist in den in lit. b) und c) genannten Fällen nur möglich, soweit die Löschung die Verwirklichung der Ziele dieser Verarbeitungen unmöglich macht oder ernsthaft beeinträchtigt. [3]Eine Löschung von Daten unterbleibt auch in anderen gesetzlich geregelten Fällen. [4]In diesen Fällen wird die Verarbeitung dieser Daten nach dem Grundsatz der Datenminimierung eingeschränkt.

VIII. EINHALTUNG UND KONTROLLE

Art. 26 Verantwortlichkeit

(1) Die Unternehmen gewährleisten als Verantwortliche, dass die Anforderungen des Datenschutzes und der Datensicherheit beachtet werden.

(2) [1]Beschäftigte, die mit der Verarbeitung personenbezogener Daten betraut sind, werden zur Vertraulichkeit hinsichtlich personenbezogener Daten, zur Einhaltung des Datenschutzes und der diesbezüglichen Weisungen des Unternehmens sowie zur Wahrung gesetzlicher Geheimhaltungspflichten auch über das Ende des Beschäftigungsverhältnisses hinaus verpflichtet. [2]Sie werden darüber unterrichtet, dass Verstöße gegen datenschutzrechtliche Vorschriften auch als Ordnungswidrigkeit geahndet oder strafrechtlich verfolgt werden und Schadensersatzansprüche nach sich ziehen können.

Art. 27 Datenschutz-Folgenabschätzung

(1) [1]Die Unternehmen prüfen die Erforderlichkeit einer Datenschutz-Folgenabschätzung (Schwellwertanalyse) und nehmen diese auch vor, soweit die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. [2]Eine Datenschutz-Folgenabschätzung ist insbesondere in folgenden Fällen erforderlich:

a) Verfahren mit automatisierten Einzelfallentscheidungen, die sich auf Verfahren zur systematischen und umfassenden Auswertung mehrerer persönlicher Merkmale der betroffenen Personen stützen, wenn sie eine Rechtswirkung gegenüber den be-

troffenen Personen entfalten oder diese in ähnlicher Weise erheblich beeinträchtigen, wie beispielsweise Verfahren zur automatisierten Risiko- oder Leistungsprüfung.

b) Verfahren mit umfangreichen Verarbeitungen besonderer Kategorien von personenbezogenen Daten, zum Beispiel Verfahren zur Risiko- oder Leistungsprüfung in der Krankenversicherung, zur Risikoprüfung in der Lebensversicherung oder zur Leistungsprüfung in der Berufsunfähigkeitsversicherung oder

c) Verfahren zur Prämienberechnung unter Verwendung verhaltensbasierter Daten betroffener Personen (z. B. für sog. Telematiktarife in der Kraftfahrtversicherung oder mit Daten aus Wearables).

(2) [1]Die Entscheidung darüber, ob eine Datenschutz-Folgenabschätzung vorgenommen wird oder nicht und die Gründe dafür werden dokumentiert. [2]Die Unternehmen stellen durch geeignete organisatorische Maßnahmen sicher, dass bei der Durchführung der Datenschutz-Folgenabschätzungen der Rat der Datenschutzbeauftragten eingeholt wird.

Art. 28 Datenschutzbeauftragte

(1) [1]Die Unternehmen oder eine Gruppe von Versicherungs- und Finanzdienstleistungsunternehmen benennen entsprechend den gesetzlichen Vorschriften Datenschutzbeauftragte.

(2) [1]Die Datenschutzbeauftragten überwachen weisungsunabhängig die Einhaltung der Datenschutz-Grundverordnung und anderer datenschutzrechtlicher Vorschriften und dieser Verhaltensregeln einschließlich der im Unternehmen bestehenden Konzepte für den Schutz personenbezogener Daten. [2]Sie werden zu diesem Zweck vor der Einrichtung oder nicht nur unbedeutenden Veränderung eines Verfahrens zur Verarbeitung personenbezogener Daten frühzeitig unterrichtet und wirken hieran beratend mit. [3]Dazu können sie in Abstimmung mit der jeweiligen Unternehmensleitung alle Unternehmensbereiche zu den notwendigen Datenschutzmaßnahmen veranlassen. [4]Insoweit haben sie ungehindertes Kontrollrecht im Unternehmen. [5]Die Datenschutzbeauftragten berichten unmittelbar der höchsten Managementebene des Unternehmens.

(3) [1]Daneben können sich alle betroffenen Personen jederzeit mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit auch an die Beauftragten für den Datenschutz wenden. [2]Anfragen, Ersuchen und Beschwerden werden vertraulich im Sinne von § 6 Abs. 5 Satz 2 BDSG und Art. 38 Abs. 5 DSGVO behandelt. [3]Die für die Kontaktaufnahme erforderlichen Daten werden in geeigneter Form veröffentlicht und der Aufsichtsbehörde mitgeteilt.

(4) Die Datenschutzbeauftragten können sich jederzeit mit der jeweils zuständigen Datenschutzaufsichtsbehörde vertrauensvoll beraten und stehen der Datenschutzaufsichtsbehörde in allen Angelegenheiten des Datenschutzes als Ansprechpartner zur Verfügung.

Art. 29 Beschwerden und Reaktion bei Verstößen

(1) [1]Die Unternehmen beantworten Beschwerden von Versicherten oder sonstigen betroffenen Personen wegen Verstößen gegen datenschutzrechtliche Regelungen sowie diese Verhaltensregeln unverzüglich, in jedem Fall aber innerhalb eines Monats oder geben innerhalb dieser Frist einen Zwischenbescheid. [2]Ein Bericht über die ergriffenen Maßnahmen kann auch noch bis zu drei Monaten nach Antragstellung erteilt werden, wenn

diese Fristverlängerung um weitere zwei Monate unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. [3]Die für die Kontaktaufnahme erforderlichen Daten werden in geeigneter Form bekannt gegeben. [4]Kann der verantwortliche Fachbereich nicht zeitnah Abhilfe schaffen, hat er sich umgehend an den Datenschutzbeauftragten zu wenden.

(2) [1]Die Geschäftsführungen der Unternehmen werden bei begründeten Beschwerden Abhilfe schaffen. [2]Sollte dies einmal nicht der Fall sein, teilen sie dies den betroffenen Personen unter Benennung der zuständigen Aufsichtsbehörde mit. [3]Die Datenschutzbeauftragten können sich an die zuständige Datenschutzaufsichtsbehörde wenden.

IX. ÜBERWACHUNG DER EINHALTUNG DER VERHALTENSREGELN

Art. 29a Überwachungsstelle

(1) [1]Die Überwachung der Einhaltung dieser Verhaltensregeln wird von einer unabhängigen Überwachungsstelle durchgeführt, die über das geeignete Fachwissen hinsichtlich des Gegenstandes dieser Verhaltensregeln verfügt und von der zuständigen Datenschutzaufsichtsbehörde zu diesem Zweck nach Art. 41 DSGVO akkreditiert wurde. [2]Ihre Aufgaben und Befugnisse ergeben sich aus diesen Verhaltensregeln.

(2) [1]Der GDV richtet eine Überwachungsstelle ein oder betraut eine geeignete Stelle mit der Aufgabe. [2]Sofern eine verbandsinterne Überwachungsstelle eingerichtet wird, ist diese bis einschließlich unterhalb der Geschäftsleitungsebene von den übrigen Bereichen des GDV zu trennen.

Art. 29b Personelle Ausstattung, Zuverlässigkeit und fachliche Eignung

(1) [1]Die Überwachungsstelle hat eine Leitung. [2]Die Leitung ist für alle Überwachungstätigkeiten verantwortlich und repräsentiert die Überwachungsstelle nach außen.

(2) [1]Bevor die Position der Leitung der Überwachungsstelle erstmalig besetzt wird und vor jedem Wechsel wird der GDV mindestens vier Wochen zuvor darüber informiert und erhält Gelegenheit zur Stellungnahme. [2]Etwaige sachlich begründete Einwände des GDV sind zu beachten, insbesondere wenn eine vorgesehene Person nicht die nach diesen Verhaltensregeln erforderliche Zuverlässigkeit oder fachliche Eignung nachgewiesen hat. [3]Das Gleiche gilt, wenn die Neutralität der Person in Frage steht oder das Vertrauensverhältnis zwischen dieser Person und der Versicherungsbranche gestört ist.

(3) [1]Die in der Überwachungsstelle tätigen Personen müssen zuverlässig sein und einzeln oder gemeinsam über die zur Wahrnehmung ihrer Tätigkeit erforderliche fachliche Eignung verfügen. [2]Die Überwachungsstelle muss Expertise in folgenden Bereichen haben:

- fundierte Kenntnis der Datenverarbeitungsprozesse in der Versicherungswirtschaft sowie Kenntnisse des Versicherungsrechts,
- sehr gute rechtliche und praktische Kenntnis im Bereich des Datenschutzes, einschließlich technischer und organisatorischer Maßnahmen,
- Kenntnisse im Bereich der Risikobewertung,
- Ausbildung oder praktische Erfahrung im Bereich von Überwachungstätigkeiten.

(4) [1]Die Überwachungsstelle kann bei kurzfristigem und unvorhergesehenem außergewöhnlichem Anfall von Aufgaben, den sie in absehbarer Zeit nicht bewältigen kann, z. B. bei unvorhergesehenem Beschwerdeaufkommen oder unaufschiebbarem Prüfungsbedarf sowie in besonders gelagerten Fällen bei der Erfüllung ihrer Überwachungsaufgaben – soweit erforderlich – durch externes Fachpersonal unterstützt werden. [2]Das externe Fachpersonal wird von der Leitung der Überwachungsstelle sorgfältig ausgewählt. [3]Für das externe Fachpersonal gelten die gleichen Anforderungen wie für die Überwachungsstelle selbst. [4]Darüber hinaus darf die Überwachungsstelle in besonders gelagerten Fällen ausnahmsweise externe Experten mit der Vornahme einzelner Untersuchungshandlungen beauftragen (z. B. mit Gutachten oder bei einem geringfügigen Personalmehrbedarf). [5]Für einzelne Aufgaben, insbesondere die Entscheidung über begründete Beschwerden und Maßnahmen, kann auch ein aus mehreren fachkundigen Personen bestehendes Komitee eingesetzt werden. [6]Externe Experten geben in jedem Fall nur eine fachliche Einschätzung ab. [7]Bewertungen und endgültige Entscheidungen werden von der Überwachungsstelle getroffen.

(5) Für rein administrativeTätigkeiten, die sich weder auf die Überwachungstätigkeit auswirken noch Einfluss auf die Unabhängigkeit der Überwachungsstelle haben, z. B. Buchhaltung, Gehaltsabrechnungen, Betrieb der IT, können Mitarbeiter des Trägers der Überwachungsstelle oder Dienstleister eingesetzt werden.

Art. 29c Unabhängigkeit und Vermeidung von Interessenkonflikten

(1) [1]Die Überwachungsstelle ist bei der Durchführung ihrer Aufgaben von dem GDV und den zu überwachenden Unternehmen weisungsfrei und unabhängig in rechtlicher, wirtschaftlicher, personeller und tatsächlicher Hinsicht, sowohl gegenüber den überwachten Unternehmen, dem GDV als Inhaber der Verhaltensregeln als auch gegenüber der gesamten Versicherungsbranche als Sektor, für den die Verhaltensregeln gelten sollen. [2]Die Überwachungsstelle identifiziert und beseitigt Gefahren für ihre Unabhängigkeit frühzeitig und fortlaufend.

(2) Unabhängigkeit und Weisungsfreiheit werden insbesondere gewährleistet durch

a) eine feste Amtszeit des Leiters/der Leiterin der Überwachungsstelle von 5 Jahren. Eine zweite Amtszeit ist möglich. Ein vorzeitiges Ende der Amtszeit durch freiwillige Niederlegung des Amtes oder Abberufung aus wichtigem Grund bleibt möglich. Ein wichtiger Grund, der die Abberufung der Leitung der Überwachungsstelle rechtfertigt, liegt insbesondere vor, wenn die für die Überwachungsstelle zuständige Datenschutzaufsichtsbehörde die Akkreditierung nach Art. 41 Abs. 5 DSGVO widerrufen hat oder bei groben und offensichtlichen Verstößen der Leitung gegen ihre Verpflichtungen oder Verfehlungen, die das Ansehen der Überwachungsstelle schwer beeinträchtigen.

b) die Möglichkeit der Überwachungsstelle, die ihr für die Überwachungstätigkeit zur Verfügung gestellten Mittel im Rahmen ihrer Aufgaben frei einzusetzen,

c) die Möglichkeit der Überwachungsstelle, die mit der Überwachung Beschäftigten eigenverantwortlich auszuwählen,

d) die vollumfängliche Freiheit der Überwachungsstelle bei ihren fachlichen Entscheidungen im Rahmen des geltenden Rechts,

e) die Freiheit der Überwachungsstelle und ihrer Mitarbeitenden oder Beauftragten von Sanktionen des GDV und der Mitgliedsunternehmen in Folge der Wahrnehmung ihrer Aufgaben.

(3) [1]Die mit der Überwachung betrauten Personen unterliegen nur den Weisungen der Leitung der Überwachungsstelle. [2]Weder sie noch die Leitung dürfen für den GDV oder ein zu überwachendes Unternehmen tätig sein.

(4) [1]Die Überwachungsstelle erfüllt ihre Aufgaben frei von Interessenkonflikten. [2]Zur Vermeidung von Interessenkonflikten identifiziert und dokumentiert die Überwachungsstelle Situationen, die in einen Interessenskonflikt münden können. [3]Sie trifft geeignete Maßnahmen, um das Auftreten von Interessenskonflikten zu verhindern.

Art. 29d Allgemeine Aufgaben und Befugnisse der Überwachungsstelle

(1) Die Überwachungsstelle bewertet, ob Unternehmen, die den Verhaltensregeln beitreten wollen, diese anwenden können.

(2) [1]Die Überwachungsstelle überwacht die Einhaltung dieser Verhaltensregeln durch die den Verhaltensregeln beigetretenen Unternehmen. [2]Dazu überprüft sie stichprobenartig jährlich eine angemessene Anzahl von Unternehmen. [3]Darüber hinaus kann sie bei entsprechenden Anhaltspunkten die Einhaltung dieser Verhaltensregeln durch das jeweilige Unternehmen anlassbezogen überprüfen. [4]Die Überprüfung kann sich auf einen oder mehrere Prüfungsschwerpunkte beziehen.

(3) [1]Sofern sich aus der Beschwerdebearbeitung mögliche Schwachstellen bei der Anwendung dieser Verhaltensregeln ergeben, sollen diese auch im Rahmen der nachfolgenden Prüfungen berücksichtigt werden. [2]Anhaltspunkte für eine anlassbezogene Prüfung eines Unternehmens liegen vor, wenn in Bezug auf das konkrete Unternehmen unter Berücksichtigung der bei diesem vorliegenden besonderen Umstände, wie z. B. seiner Größe, eine deutlich erhöhte Anzahl von Beschwerden oder Datenpannen, die auf strukturelle Defizite bei der Anwendung der Verhaltensregeln hindeuten, festgestellt wurden.

(4) Die Datenschutzbeauftragten der Unternehmen werden bei der Überwachung rechtzeitig einbezogen.

(5) [1]Die Überwachungsstelle trägt zur Überprüfung bei, ob die Verhaltensregeln praxistauglich, hinreichend präzise und verständlich sind, den Regelungsbedarf abdecken und von der Praxis akzeptiert werden. [2]Sie informiert den GDV über wesentliche Erkenntnisse aus ihrer Überwachungstätigkeit zeitnah, aber mindestens einmal jährlich. [3]Sie kann dem GDV zudem im Rahmen jeder Evaluation der Verhaltensregeln eine Einschätzung zur Geeignetheit der Verhaltensregeln auf Grundlage der Ergebnisse ihrer Überwachungstätigkeit geben.

Art. 29e Beschwerdebearbeitung

(1) [1]Die Überwachungsstelle bearbeitet Beschwerden über Verletzungen dieser Verhaltensregeln oder über die Art und Weise, in der diese von den Unternehmen angewendet werden oder wurden, bevorzugt vor ihren anderen Aufgaben. [2]Beschwerden können von jeder Person eingereicht werden, die eine Verletzung ihrer Rechte durch einen Verstoß gegen diese Verhaltensregeln geltend macht. [3]Anonym eingereichte Beschwerden werden von der Überwachungsstelle bearbeitet, soweit sich daraus nachvollziehbare Hinweise für Verstöße gegen diese Verhaltensregeln ergeben.

(2) [1]Die Überwachungsstelle begründet ihre Entscheidung. [2]Sie dokumentiert alle eingegangenen Beschwerden und ihre getroffenen Maßnahmen.

(3) [1]Die Überwachungsstelle macht die Verfahren und Strukturen für den Umgang mit Beschwerden in geeigneter Form transparent. [2]Die diesen Verhaltensregeln beigetretenen Unternehmen geben die Möglichkeit der Beschwerde bei der Überwachungsstelle und deren Kontaktdaten in geeigneter Form bekannt.

(4) [1]Die Überwachungsstelle befasst sich mit der Beschwerde unter Berücksichtigung der spezifischen Umstände des Einzelfalls. [2]Sie informiert Beschwerdeführer innerhalb von drei Monaten nach Eingang der Beschwerde über den Ausgang des Beschwerdeverfahrens bzw. den derzeitigen Verfahrensstand.

(5) [1]Für den Beschwerdeführer ist die Bearbeitung der Beschwerde gebührenfrei. [2]Bei offenkundig unbegründeten oder missbräuchlichen Beschwerden kann die Überwachungsstelle von der beschwerdeführenden Person ein angemessenes Entgelt verlangen oder sich weigern, auf die Beschwerde hin tätig zu werden. [3]Missbräuchliche Beschwerden liegen z. B. bei häufiger Wiederholung eines identischen Beschwerdegegenstandes bei identischer Sach- und Rechtslage durch die gleiche Person vor. [4]Die Überwachungsstelle dokumentiert ihre Gründe für die Annahme des offenkundig unbegründeten oder missbräuchlichen Charakters der Beschwerde.

(6) [1]Das Nähere zum Beschwerdeverfahren regelt die Beschwerdeordnung der Überwachungsstelle. [2]Die Beschwerdeordnung wird an geeigneter Stelle mit den Verhaltensregeln veröffentlicht.

Art. 29f Geeignete Maßnahmen der Überwachungsstelle bei Verstößen

(1) [1]Hat die Überwachungsstelle bei einer Prüfung oder im Rahmen eines Beschwerdeverfahrens einen Verstoß gegen diese Verhaltensregeln festgestellt, verlangt sie die Umsetzung geeigneter Garantien zur Beendigung des Verstoßes binnen eines angemessenen Zeitraums. [2]Geeignete Garantien können z. B. die Vorlage eines Konzeptes für eine mit den Verhaltensregeln konforme Umstellung von Verarbeitungsprozessen, eine Änderung von Verarbeitungsvorgängen, die Verbesserung technischer oder organisatorischer Maßnahmen oder die Schulung der zuständigen Mitarbeiter sein.

(2) [1]Sofern ein Unternehmen keine geeigneten Garantien bietet oder den festgestellten Verstoß gegen diese Verhaltensregeln wiederholt oder fortsetzt, kann die Überwachungsstelle geeignete Maßnahmen gegenüber dem Unternehmen ergreifen. [2]Das Gleiche gilt, wenn die Überwachungsstelle innerhalb des letzten halben Jahres bereits mehr als drei unterschiedliche Verstöße oder einen schwerwiegenden Verstoß gegen diese Verhaltensregeln festgestellt hat.

(3) Geeignete Maßnahmen sind förmliche Maßnahmen zu dem Zweck, den Verstoß abzustellen und eine künftige Wiederholung zu vermeiden.

(4) Geeignete Maßnahmen sind:

a) förmliche Aufforderungen zum Abstellen des Verstoßes,

b) Meldung des Verstoßes bei der Geschäftsleitung und dem Datenschutzbeauftragten des Unternehmens,

c) förmliche Verwarnungen,

d) die Androhung des Ausschlusses von diesen Verhaltensregeln,

e) der vorläufige Ausschluss von diesen Verhaltensregeln sowie

f) bei wiederholten Verstößen der endgültige Ausschluss von diesen Verhaltensregeln, sofern durch die unter a) – e) aufgeführten Maßnahmen dem Verstoß nicht abgeholfen werden kann.

(5) [1]Geeignete Maßnahmen müssen wirksam, verhältnismäßig und angemessen sein. [2]Bevor eine geeignete Maßnahme ergriffen wird, hört die Überwachungsstelle das Unternehmen an. [3]Die Überwachungsstelle begründet die geeigneten Maßnahmen schriftlich. [4]Zwischen den in Abs. 4 lit. a) bis f) genannten Maßnahmen besteht grundsätzlich ein Stufenverhältnis in der Reihenfolge ihrer Auflistung. [5]Sofern die Wirksamkeit, Geeignetheit und Verhältnismäßigkeit der Maßnahmen nicht in Frage steht, soll die Überwachungsstelle bei der Entscheidung über Maßnahmen dem Stufenverhältnis folgen.

(6) Die Verfahrensordnung regelt, unter welchen Voraussetzungen ein vorläufiger Ausschluss von den Verhaltensregeln endet.

Art. 29g Vertraulichkeit

(1) Die Überwachungsstelle behandelt alle Informationen, die sie bei Ausübung ihrer Tätigkeit erhält, vertraulich.

(2) Die Pflicht zur Geheimhaltung gilt nicht, sofern die Überwachungsstelle zur Offenlegung der Informationen gesetzlich verpflichtet oder von dem jeweils überwachten Unternehmen bzw. den Betroffenen ausdrücklich berechtigt wurde.

(3) [1]Die Pflicht der Überwachungsstelle zur Vertraulichkeit und Geheimhaltung bezieht sich insbesondere auf die personenbezogenen Daten der Betroffenen, Privatgeheimnisse nach § 203 StGB und Geschäftsgeheimnisse der Unternehmen. [2]Die Pflicht zur Vertraulichkeit und Geheimhaltung gilt für alle für die Überwachungsstelle tätigen Personen auch nach Beendigung ihrer Tätigkeit. [3]Die Überwachungsstelle verpflichtet darüber hinaus von ihr für die Erfüllung ihrer Aufgaben ggf. hinzugezogene Dritte entsprechend zur Verschwiegenheit.

(4) [1]Die Überwachungsstelle veröffentlicht keine Aussagen über konkrete Prüfungs- oder Beschwerdeverfahren. [2]Die Verpflichtung zur Information der für die überwachten Unternhemen zuständigen Datenschutzaufsichtsbehörde nach Art. 41 Abs. 4 Satz 2 DSGVO bleibt unberührt.

(5) [1]Sofern die zu veröffentlichenden Informationen einen Rückschluss auf die Identität der überwachten Unternehmen bzw. die Betroffenen zulassen, müssen diese vor jeder Offenlegung informiert werden und Gelegenheit zur Stellungnahme erhalten. [2]Grundsätzlich muss für die Stellungnahme eine Frist von mindestens einem Monat vor der geplanten Offenlegung gewährt werden.

Art. 29h Dokumentation und Unterrichtung

(1) Die Überwachungsstelle dokumentiert ihre Überwachungstätigkeit sowie die Bearbeitung jeder Beschwerde.

(2) [1]Sie erstellt einmal jährlich einen zusammenfassenden Bericht über die wesentlichen Ergebnisse ihrer Tätigkeit. [2]Die Überwachungsstelle stellt den Bericht der für sie zuständigen Datenschutzaufsichtsbehörde, den für die betroffenen Unternehmen zuständigen

Datenschutzaufsichtsbehörden und dem GDV zur Verfügung. [3]Über Maßnahmen nach Artikel 29f Abs. 4 lit. c), e) und f) dieser Verhaltensregeln informiert die Überwachungsstelle die für das betroffene Unternehmen zuständige Datenschutzaufsichtsbehörde und den GDV unverzüglich. [4]Über einen schwerwiegenden Verstoß informiert die Überwachungsstelle ebenfalls die für das betroffene Unternehmen zuständige Datenschutzaufsichtsbehörde. [5]Die Überwachungsstelle veröffentlicht den endgültigen Ausschluss von Unternehmen von den Verhaltensregeln.

Art. 29i Substanzielle Veränderungen

[1]Die Überwachungsstelle meldet dem GDV und der für sie zuständigen Datenschutzaufsichtsbehörde erhebliche Veränderungen, die sich auf die Wahrnehmung der Aufgaben der Überwachungsstelle auswirken können, unverzüglich. [2]Sie informiert den GDV insbesondere unverzüglich über einen Widerruf der Akkreditierung nach Art. 41 Abs. 5 DSGVO oder wenn die für die Überwachungsstelle zuständige Datenschutzaufsichtsbehörde gegen sie ein Bußgeld nach Art. 83 Abs. 4 DSGVO verhängt bzw. dies angekündigt hat.

Art. 29j Finanzierung der Überwachung

[1]Die Überwachungsstelle erhält von den überwachten Unternehmen die erforderlichen finanziellen Mittel, die eine angemessene Überwachungstätigkeit und ihre langfristige Stabilität sicherstellen. [2]Das Ausscheiden einzelner oder mehrerer Unternehmen darf ihre Finanzierung nicht gefährden.

Art. 29k Verfahrensordnung

Weitere Details zu der Überwachungsstelle und ihren Verfahren regelt die Verfahrensordnung.

X. FORMALIA

Art. 30 Beitritt

(1) [1]Die Unternehmen, die diesen Verhaltensregeln beigetreten sind, verpflichten sich zu deren Einhaltung ab dem Zeitpunkt des Beitritts. [2]Der Beitritt der Unternehmen wird vom GDV dokumentiert und in geeigneter Form bekanntgegeben.

(2) Versicherungsnehmer, deren Verträge vor dem Beitritt des Unternehmens zu diesen Verhaltensregeln bereits bestanden, werden über den Beitritt zu diesen Verhaltensregeln über den Internetauftritt des Unternehmens sowie spätestens mit der nächsten Vertragspost in Textform informiert.

(3) [1]Hat ein Unternehmen seinen Beitritt zu diesen Verhaltensregeln erklärt, ist die jeweils gültige Fassung wirksam. [2]Eine Rücknahme des Beitritts ist jederzeit möglich durch Erklärung gegenüber dem GDV. [3]Wenn ein Unternehmen die Rücknahme des Beitritts erklärt, wird dies durch die Löschung des Unternehmens in der Beitrittsliste vom GDV dokumentiert und in Form einer aktualisierten Beitrittsliste in geeigneter Weise bekannt gegeben. [4]Das Unternehmen wird zudem die für das Unternehmen zuständige Datenschutzaufsichtsbehörde und die Versicherten über die Rücknahme informieren.

Art. 31 Evaluierung

Diese Verhaltensregeln werden bei jeder ihren Regelungsgehalt betreffenden Rechtsänderung in Bezug auf diese, spätestens aber alle fünf Jahre insgesamt evaluiert.

Art. 32 Inkrafttreten

[1]Diese Fassung der Verhaltensregeln gilt ab dem [Datum der Genehmigung] und ersetzt den Datenschutzkodex vom 1. August 2018. [2]Mit der Genehmigung gelten alle Rechtsfolgen, die die DSGVO an nach Art. 40 Abs. 5 DSGVO genehmigte Verhaltensregeln knüpft. [3]Soweit zur Einhaltung dieser Verhaltensregeln technische Änderungen der Datenverarbeitungsverfahren in den Unternehmen erforderlich sind, setzen die Unternehmen diese zum schnellstmöglichen Zeitpunkt um.