Versicherungsverband Österreich

Branchenstandard Datenschutz der österreichischen Versicherungswirtschaft

Inhaltsverzeichnis

1. Einleitung

Die Datenschutz-Grundverordnung (DSGVO) regelt und vereinheitlicht das gesamte Datenschutzrecht in der Europäischen Union und ist - auch in Österreich - direkt anwendbar. Die DSGVO enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten.
Die österreichische Versicherungswirtschaft verarbeitet personenbezogene Daten, insbesondere bei der Beratung und Betreuung von *Versicherungsnehmern*, sowie bei der Antrags-, Vertrags- und Leistungsabwicklung. Hierfür ist eine Vielzahl von gesetzlichen Bestimmungen anwendbar.

Der Branchenstandard versteht sich als branchenspezifische Auslegung und Konkretisierung der datenschutzrechtlichen Bestimmungen für die Belange der Versicherungswirtschaft in der Praxis und durch seine konkretisierende Wirkung auch als Schutzmaßnahme für die *Kunden*. Er versteht sich nicht als Mindestanforderung an die Datenverarbeitungsprozesse in der Versicherungswirtschaft, sondern er zeichnet ein typisierendes Bild der versicherungsspezifischen Datenverarbeitungen.
Der Schutz der Daten ihrer *Kunden*, deren Privatsphäre sowie die Sicherheit der Datenverarbeitung sind für die österreichische Versicherungswirtschaft ein selbstverständliches Kernanliegen. Sie ist sich ihrer Stellung und Verantwortung bewusst und kommt den Grundsätzen der DSGVO, des Datenschutzgesetzes (DSG), sowie allen versicherungsspezifischen gesetzlichen Vorschriften in besonderer Weise nach, um das Vertrauen ihrer *Kunden* umfassend sicherstellen zu können.
Aus diesen Gründen bekennt sich die österreichische Versicherungswirtschaft als Mehrwert für ihre *Kunden* einvernehmlich und freiwillig im Rahmen der folgenden Verhaltensregeln zu einer gemeinsamen und wirksamen Anwendung der datenschutzrechtlichen Erfordernisse und Verpflichtungen unter Berücksichtigung der Besonderheiten der Branche.
Dieser Branchenstandard wurde vom Verband der Versicherungsunternehmen Österreichs (VVO) in Zusammenarbeit mit seinen Mitgliedern ausgearbeitet. Dabei wurde besonderes Augenmerk auf transparente und verständliche Formulierungen zum bestmöglichen Verständnis für *Versicherungsnehmer* gelegt. Als Regelungen speziell für Versicherungen erfassen sie die wichtigsten Verarbeitungen personenbezogener Daten, welche Versicherungen vor, während und nach der Vertragsbeziehung zu ihren *Kunden* vornehmen.

Haben Unternehmen bereits eigene besonders datenschutzfreundliche Regelungen getroffen, behalten diese selbstverständlich parallel zu diesem Branchenstandard ihre Gültigkeit.
Dieser Branchenstandard wurde bei der für die Einhaltung der datenschutzrechtlichen Bestimmungen zuständigen Aufsichtsbehörde (Datenschutzbehörde) eingereicht und bescheidmäßig genehmigt.

Erklärung des kollektiven Risikoausgleichs
Zum Verständnis der Verarbeitung personenbezogener Daten in der Versicherungswirtschaft ist es notwendig, auch die Grundsätze des Versicherungsgeschäftes zu verstehen. Jeder Versicherung liegt das Prinzip der kollektiven Risikoübernahme zu Grunde. Dies bedeutet, dass es bei einer gemeinsamen Tragung von Risiken in einem Kollektiv zu einem *Risikoausgleich* kommt, der es der Versicherung ermöglicht, versicherungsmathematisch einen nur sehr geringen Risikoaufschlag in ihre Prämien zu kalkulieren und dennoch im Versicherungsfall auch hohe Einzelschäden abdecken zu können. Um dies zu ermöglichen ist es notwendig, ein Risiko korrekt beurteilen zu können und die entsprechenden Prämien zu verrechnen. Dabei ist zu berücksichtigen, dass Versicherungsunternehmen gem. § 110 VAG ein wirksames Risikomanagementsystem einrichten müssen, das alle erforderlichen Strategien, Prozesse und Meldeverfahren umfasst und für die *Versicherungsnehmer* sicherstellt, dass in deren Versicherungsfällen stets ausreichende Liquidität vorhanden ist. Sollten Prämien versicherungsmathematisch nicht korrekt festgesetzt werden, führt dies

zu höheren Prämien für die restliche Versicherungsgemeinschaft. Diesem Interessenausgleich trägt der Gesetzgeber im Speziellen hinsichtlich der versicherungsbezogenen Verwendung von Gesundheitsdaten in den §§ 11a bis 11d VersVG Rechnung.

2. Anwendbarkeit und Geltungsbereich

Die folgenden Verhaltensregeln dieses Branchenstandards gelten für die Verarbeitung personenbezogener Daten durch Versicherungsunternehmen im Rahmen ihrer Versicherungstätigkeiten im Inland. Nicht davon umfasst ist daher beispielsweise der Umgang mit personenbezogenen Daten von Versicherungsmitarbeitern im Rahmen ihres Anstellungsverhältnisses.

Der Branchenstandard spezifiziert die Regelungen der DSGVO und die einschlägigen datenschutzrechtlichen Bestimmungen des Versicherungsvertragsgesetzes. Bei diesen handelt es sich um die §§ 11a bis 11d VersVG, welche ausweislich der Gesetzesmaterialien als eine Rechtsvorschrift im öffentlichen Interesse gelten und die Fälle der Erhebung und Verarbeitung personenbezogener Gesundheitsdaten zur Antrags- und Leistungsfallprüfung (§ 11a VersVG), der Direktverrechnung zwischen Gesundheitsdienstleistern und Privatversicherern (§ 11b VersVG), der antrags- und leistungsfallbezogenen Datenübermittlungen (§ 11c VersV) und der Vertraulichkeit der zur Verarbeitung stehenden Daten (§ 11d VersVG) regeln. Es ist das Verständnis dieses Branchenstandards, dass diesen gesetzlichen Vorgaben bei der Verarbeitung personenbezogener Gesundheitsdaten stets Folge zu leisten ist und es wird demgemäß an den gebotenen Stellen auf diese Bestimmungen des VersVG Bezug genommen.
Es ist das Verständnis des Branchenstandards, dass der Datenschutz nur für lebende natürliche Personen greift, sodass datenschutzrechtliche Schutzbestimmungen bei Verstorbenen nicht zur Anwendung gelangen.

Die folgenden Verhaltensregeln werden von Versicherungsunternehmen angewendet, welche dem Branchenstandard durch Erklärung gegenüber dem Verband der Versicherungsunternehmen Österreichs (VVO) als koordinierende Stelle beigetreten sind. Eine Verbandsmitgliedschaft ist keine zwingende Voraussetzung für den Beitritt.
Die aktuelle Beitrittsliste wird vom Verband der Versicherungsunternehmen Österreichs (VVO) in geeigneter Form veröffentlicht.

3. Begriffsbestimmungen

Zusätzlich zu den in Art. 4 DSGVO definierten Begriffen werden fachspezifische Begriffe wie folgt definiert. Diese werden im Text durch kursive Schreibweise hervorgehoben.

Bezugsberechtigter
Die vom *Versicherungsnehmer* bestimmte Person, welche vom Versicherer in der Unfall-, Renten- oder Lebensversicherung die vereinbarte Leistung im Versicherungsfall erhält.

DSB
Österreichische Datenschutzbehörde, www.dsb.gv.at

Datenschutzinformation
Informationen über die Verarbeitung personenbezogener Daten, die der Verantwortliche der betroffenen Person gemäß Art. 12, 13 und 14 DSGVO zur Verfügung stellt.

Drittland
Ein Drittland ist ein Staat, der nicht Mitglied der EU oder des EWR (EU sowie Island, Liechtenstein, Norwegen) ist.

FMA
Finanzmarktaufsichtsbehörde, www.fma.gv.at

Geschädigter
Personen, die in der Haftpflichtversicherung Schadenersatzansprüche gegen den *Versicherungsnehmer* oder eine andere *versicherte Person* geltend machen.

GTelG - Gesundheitstelematikgesetz
Bundesgesetz betreffend Datensicherheitsmaßnahmen bei der Verarbeitung elektronischer Gesundheitsdaten und genetischer Daten (Gesundheitstelematikgesetz 2012 – GTelG 2012)

Kunden
Sammelbegriff für Rollen wie *Versicherungsnehmer*, *versicherte Person*, *Bezugsberechtigter*, *Prämienzahler*.

Mitversicherung
Eine Mitversicherung ist die Beteiligung mehrerer Versicherungsunternehmen an der Versicherung desselben Risikos.

Prämienzahler
Diejenige Person, die dem Versicherer die vereinbarte Versicherungsprämie bezahlt. Prämienzahler und *Versicherungsnehmer* müssen nicht unbedingt ident sein.

Risikoausgleich
Eine Kernaufgabe des Versicherers, bei dem der Schadeneintritt eines individuellen Risikos durch ein Kollektiv oder einen bestimmten Zeitraum nivelliert wird.

Rückversicherung
Eine Rückversicherung ist die Übertragung von Risiken von einem Versicherungs- auf ein Rückversicherungsunternehmen. Sie ermöglicht dem Erstversicherer eine Verminderung seines versicherungstechnischen Risikos.

Schadendaten
Im Zuge der Schaden- oder Leistungsfallbearbeitung verarbeitete personenbezogene Daten (z.B. Schadennummer, Schadendatum, Angaben zur Schadenursache, Beschreibung des Schadens, Schadenhöhe). Zu den Schadendaten zählen auch Gesundheitsdaten, sofern diese im Konnex zu einer Schadenfallbearbeitung stehen.

Stammdaten
Die allgemeinen personenbezogenen Daten einer betroffenen Person (z.B. Name, Geburtsdatum, Kundennummer, Adresse, E-Mail-Adresse, Telefonnummer, Bankverbindung).

TKG - Telekommunikationsgesetz (TKG 2021)
Das Telekommunikationsgesetz regelt alle rechtlichen Belange der Telekommunikation in Österreich.

VAG – Versicherungsaufsichtsgesetz
Bundesgesetz über den Betrieb und die Beaufsichtigung der Vertragsversicherung (Versicherungsaufsichtsgesetz 2016 – VAG 2016). Gemäß dem Versicherungsaufsichtsgesetz werden u.a. Betrieb, Produktgestaltung und Kapitalveranlagung von Versicherungsunternehmen in Österreich geregelt. Die Beaufsichtigung erfolgt durch die Finanzmarktaufsichtsbehörde (FMA).

Versicherte Person
Versicherungsnehmer und/oder jene Person, auf dessen Personen- oder Sachrisiko sich der vereinbarte Versicherungsschutz erstreckt.

Versicherungsnehmer
Vertragspartner des Versicherers im *Versicherungsvertrag*.

Versicherungsvermittler
Sammelbegriff für Versicherungsmakler und Versicherungsagenten.

Versicherungsvertrag
Vertrag zwischen Versicherer und *Versicherungsnehmer*, auf dessen Grundlage der Versicherer gegen Bezahlung einer Versicherungsprämie für ein bestimmtes Risiko Versicherungsschutz gewährt.

VersVG – Versicherungsvertragsgesetz
Bundesgesetz über den Versicherungsvertrag

Vertragsdaten
Im Zuge des Abschlusses und der Verwaltung eines *Versicherungsvertrags* verarbeitete personenbezogene Daten (z.B. Polizzennummer, Versicherungstarif, Vertragsbeginn und -ende, Versicherungsprämie, Versicherungssumme, Daten zum versicherten Risiko, Zahlungsart).

VVO
Verband der Versicherungsunternehmen Österreichs, www.vvo.at

4. Rollen und datenschutzrechtliche Berechtigungen in der Versicherungswirtschaft

4.1. Versicherer

4.1.1. Sind Versicherer Verantwortliche oder Auftragsverarbeiter?

Als konzessionierte Versicherungsunternehmen sind die Versicherer selbst für die Verarbeitung und den Schutz von personenbezogenen Daten ihrer *Kunden* verantwortlich. Dabei nehmen Versicherer im datenschutzrechtlichen Sinn die Funktion eines „Verantwortlichen“ ein; ihre *Kunden* sind Betroffene. Dies gilt z.B. auch dann, wenn ein Unternehmen als *Versicherungsnehmer* seine Mitarbeiter über einen Gruppenversicherungsvertrag versichert und der Versicherer dabei personenbezogene Daten der Mitarbeiter (= *versicherte Personen*) verarbeitet. Es ist daher jedenfalls nicht erforderlich, dass ein *Versicherungsnehmer* mit seinem Versicherer eine Vereinbarung über eine Auftragsverarbeitung oder gemeinsame Verantwortlichkeit abschließt.

4.1.2. Verschiedene Versicherer gemeinsam für die Verarbeitung verantwortlich?

Für gewisse Datenverarbeitungen können Versicherer als gemeinsam für die Verarbeitung Verantwortliche tätig sein. Die Versicherer informieren in ihren *Datenschutzinformationen* über das Bestehen von gemeinsamen Verantwortlichkeiten. Gemeinsame Verantwortlichkeiten können im Besonderen bei vom VVO zentral betriebenen Systemen bestehen (siehe 4.2).

4.1.3. Datenübermittlung zwischen Versicherern

Im Rahmen des Versicherungsbetriebs sind verschiedene Konstellationen denkbar, in denen Versicherer personenbezogene Daten untereinander austauschen bzw. sich gegenseitig zur Verfügung stellen. Der Austausch von Daten zwischen Versicherern kann auch über beim VVO betriebene Systeme erfolgen. Bei den nachfolgend beschriebenen typischen Konstellationen verarbeiten die (Rück-)Versicherer diese Daten jeweils als (eigenständig) Verantwortliche iSd DSGVO; die einzige Ausnahme bildet das Bonus/Malusauskunftssystem, bei dem die teilnehmenden Versicherer gemeinsam Verantwortliche sind.

4.1.3.1. Abwicklung Internationale Versicherungskarte (vormals „Grüne Karte“)

Die Kraftfahrzeug-Haftpflichtversicherung für ein in Österreich zugelassenes Fahrzeug gilt für Europa im geografischen Sinn. In fast allen europäischen Ländern gilt das amtliche österreichische Kennzeichen als Nachweis der bestehenden Haftpflichtversicherung. Trotzdem wird empfohlen, bei Auslandsreisen die sogenannte „Grüne Karte“ als Versicherungsnachweis mitzuführen (die Grüne Karte wird automatisch oder auf Anforderung vom Kfz-Haftpflichtversicherer ausgestellt). Die Daten werden dem ausländischen *Korrespondenzversicherer* bzw. dem nationalen Versicherungsbüro (in Österreich ist das der VVO) zur Verfügung gestellt.

Nach Verkehrsunfällen, die sich in einem EU-Staat oder in Island, Liechtenstein Norwegen oder der Schweiz mit einem dort zugelassenen Fahrzeug ereignen, können die Schadenersatzansprüche im Heimatland geltend gemacht werden. Jeder Kfz-Haftpflichtversicherer, der in einem solchen Staat tätig ist, muss in einem EU-Staat, Island, Liechtenstein, Norwegen oder der Schweiz einen so genannten „Schadenregulierungsbeauftragten“ (zum Beispiel eine Versicherung oder ein spezialisiertes Schadenregulierungsbüro) bekannt geben. Dieser wird im Einvernehmen mit dem zuständigen ausländischen Versicherer die Schadenersatzansprüche bearbeiten und außergerichtlich erledigen. Zum Zwecke der Schadenabwicklung ist daher die Verarbeitung und Offenlegung von personenbezogenen Daten erforderlich (Art. 6 Abs. 1 lit b DSGVO, Art. 9 Abs. 2 lit f DSGVO).

4.1.3.2. Mitversicherung

Im Falle einer *Mitversicherung* beteiligen sich mehrere Versicherer an der Versicherung desselben Risikos. In diesem Zusammenhang haftet jeder Versicherer nur für seinen Anteil an der Gesamtversicherungssumme. Es ist daher der Austausch von personenbezogenen Daten (Vertrags- und *Schadendaten*) unter den Mitversicherern zum Zweck der Vertrags- und Schadenabwicklung notwendig (Art. 6 Abs. 1 lit b DSGVO). (Mit-)Versicherer können auch Gesundheitsdaten zu Zwecken der Risikoprüfung, Vertragsverwaltung und Leistungsprüfung auf Basis einer gesetzlichen Ermächtigung an beteiligte Mitversicherer übermitteln (Art. 9 Abs. 2 lit f DSGVO iVm § 11c Abs. 1 Z 2 u § 11a Abs. 1 VersVG). Jeder Versicherer bleibt im Rahmen von Mitversicherungsverhältnissen für seine eigene Geschäftsgebarung verantwortlich und verarbeitet personenbezogene Daten als eigenständig Verantwortlicher.

4.1.3.3. Rückversicherung

Um jederzeit zur Erfüllung ihrer Verpflichtungen aus den Versicherungsverhältnissen in der Lage zu sein, geben Versicherer einen Teil ihrer Risiken aus den *Versicherungsverträgen* an Rückversicherer weiter. Zum weiteren *Risikoausgleich* bedienen sich in einigen Fällen diese Rückversicherer ihrerseits weiterer Rückversicherer.

Eine wesentliche Unterscheidung ist jene zwischen obligatorischer und fakultativer *Rückversicherung*: Bei der obligatorischen *Rückversicherung* übernimmt ein Rückversicherer einen im Rückversicherungsvertrag vorab definierten Umfang an Risiken aus dem Bestand eines Versicherers.[1] Der Rückversicherer erhält dabei im Wesentlichen lediglich anonymisierte oder pseudonymisierte Bestandsdaten des Versicherers zu Verrechnungszwecken. Nur in Ausnahmefällen erhält der Rückversicherer personenbezogene Vertrags- und *Schadendaten*, um selbst eine Prüfung eines rückversicherten Leistungsfalls durchführen zu können (z.B. bei ab einer bestimmten Schadenshöhe obligatorisch rückversicherten Großschäden). Bei der fakultativen *Rückversicherung* werden dagegen auf Einzelvertragsbasis einzelne große Risiken rückversichert. Damit der Rückversicherer prüfen kann, ob und zu welchen Konditionen er ein einzelnes Großrisiko fakultativ übernehmen möchte, und damit er im Versicherungsfall selbst eine Einschätzung seiner Leistungspflicht vornehmen kann, ist es notwendig, dass der Versicherer die für diese Prüfungen erforderlichen Vertrags- und *Schadendaten* an ihn weiterleitet.

Zusammengefasst kommt es also v.a. im Großrisiken- und Großschadenbereich zu einer Übermittlung von personenbezogenen Vertrags- und *Schadendaten* an Rückversicherer (Art. 6 Abs. 1 lit b DSGVO). In der Personenversicherung können dabei auch Gesundheitsdaten auf Basis einer gesetzlichen Ermächtigung an den Rückversicherer übermittelt werden (Art. 9 Abs. 2 lit f DSGVO iVm § 11c Abs. 1 Z 2 u § 11a Abs. 1 VersVG). Im Rahmen ihrer Rückversicherungstätigkeit sind Rückversicherer Verantwortliche für ihre eigenen Datenverarbeitungen.

4.1.3.4. Teilungsabkommen

Teilungsabkommen sind Vereinbarungen zwischen Versicherern untereinander zur Teilung von Schadenleistungen (z. B. das Abkommen zwischen KFZ Haftpflicht- und Kaskoversicherer), wonach bei einem Schaden – unabhängig von der Verschuldensfrage – die Kaskoversicherung einen Teil des Schadens übernimmt. Zum Zweck dieser Schadenabwicklung ist der Austausch von personenbezogenen Daten unter Versicherern notwendig (Art. 6 Abs. 1 lit b DSGVO).

4.1.3.5. Regress

Soweit *versicherte Personen* ihre Pflichten und Obliegenheiten verletzen, ist es mitunter möglich, dass sich Versicherer die erbrachte Entschädigungsleistung beim Schadenverursacher zurückholen (Regress). Gleiches gilt bei Leistungen aus der Solidarhaftung.

Es ist z.B. erforderlich, zur Verfolgung von etwaigen Rechtsansprüchen (Art. 6 Abs. 1 lit f bzw. Art. 9 Abs. 2 lit f DSGVO) gegenüber dem Versicherer des Schadenverursachers oder bei Mehrfachversicherungen Informationen mit den beteiligten Versicherern auszutauschen.

---

[1] Beispiel 1 (Quoten-Rückversicherung): Der Versicherer gibt eine bestimmte Quote seines KFZ-Haftpflichtbestands an den Rückversicherer weiter. Der Rückversicherer erhält vom Versicherer einen entsprechenden Anteil der in dieser Sparte verrechneten Versicherungsprämien und ersetzt diesem auch einen entsprechenden Anteil an Versicherungsleistungen.

Beispiel 2 (Einzel-Schadenexzedent-Rückversicherung): Der Rückversicherer übernimmt in der Gebäudeversicherung für alle Schadensfälle ab einer bestimmten Schadenshöhe (Großschäden) das alleinige Risiko und erhält hierfür vom Versicherer eine Rückversicherungsprämie.

4.1.3.6. Bonus/Malus System

Kfz-Versicherer nutzen die beim Verband der Versicherungsunternehmen Österreichs (VVO) betriebene Datenaustauschplattform „Bonus/Malus-Auskunftssystem“ (siehe 4.2.6.) zum Zweck der Prämieneinstufung in der Kfz-Haftpflichtversicherung. Die an diesem System teilnehmenden KFZ-Versicherer sind gemäß DSGVO gemeinsame Verantwortliche und der VVO nimmt die Rolle des Auftragsverarbeiters war. Die Eintragung in dieses System erfolgt im berechtigten Interesse des jeweiligen KFZ-Versicherers zur Verwirklichung einer Risikomanagementmaßnahme iSd § 110 VAG. Jeder *Versicherungsnehmer* wird bereits bei Vertragsabschluss über das Bestehen und den Zweck des Bonus/Malus-Auskunftssystems und die Kontaktdaten des VVO informiert.
Einmeldungen erfolgen, um eine korrekte Einstufung im Bonus/Malus System der Kfz-Haftpflichtversicherung zu ermöglichen. Durch dieses System wird gewährleistet, dass unfallfrei bleibende *Versicherungsnehmer* eine geringere Versicherungsprämie erhalten. Dadurch wird ein schadenvermeidender Fahrstil der *Versicherungsnehmer* belohnt, was im Interesse einer für alle leistbaren flächendeckenden Kfz-Haftpflichtversicherung sowie selbstverständlich aller am Verkehr teilnehmenden Personen ist.
Der Kfz-Versicherer übermittelt dazu nach der Beendigung einer Kfz-Haftpflichtversicherung ohne Abschluss eines Nachfolgevertrages beim selben Versicherer den Namen, das Geburtsdatum und die Anschrift des *Versicherungsnehmers*, die Polizzennummer des *Versicherungsvertrages*, das Kfz- Kennzeichen des bisher versicherten Kraftfahrzeuges, die Fahrgestellnummer, das Datum des Beginns und der Beendigung des *Versicherungsvertrages* mit Bonus/Malus-Stufe, Beobachtungszeitraum, Schadendatum.
Die Daten werden vom nachfolgenden Versicherer nur im Antragsfall abgefragt, wenn ein *Versicherungsnehmer* einen Neuvertrag ohne Vorvertrag beim selben Versicherer abschließt, um die Bonus/Malus-Stufe aus dem Vorvertrag zu übernehmen. Nach Ablauf von drei Jahren ab Beendigung des *Versicherungsvertrages* werden die Daten gelöscht.

4.2. Rolle des VVO

Dem Verband der Versicherungsunternehmen (VVO) obliegt satzungsgemäß die Interessenvertretung der österreichischen Versicherer. Dabei nimmt der VVO keine Zweck- und Mittelfestlegung der operativen Datenverarbeitungen der Versicherer vor, sondern er unterstützt diese bei diesen Tätigkeiten. In rollenbezogener Betrachtung verarbeitet der VVO daher als datenschutzrechtlicher Auftragsverarbeiter gemäß Art. 4 Z 8 DSGVO personenbezogene Daten im Auftrag der Versicherungswirtschaft. Die Verarbeitungsvorgänge werden entweder jeweils im Auftrag eines verantwortlichen Versicherers gemäß Art. 4 Z 7 DSGVO oder im Auftrag mehrerer verantwortlicher Versicherer als gemeinsame Verantwortliche durchgeführt. Im Folgenden wird eine schematische Rollenverteilung hinsichtlich der Datenverarbeitungen des VVO wiedergegeben, wobei es unter den konkreten Umständen zu Abweichungen von diesem Rollenschema auf Seite der Verantwortlichen kommen kann, so etwa wenn mehrere Versicherer als gemeinsam Verantwortliche eine Datenaustauschplattform betreiben. Davon unberührt bleibt, dass der VVO stets die Rolle des Auftragsverarbeiters bekleidet.

Bezeichnung	**Zweck der Auftragsverarbeitung**	Jeweils für einen verantwortlichen Versicherer	Für gemeinsam verantwortliche Versicherer
LET-Tilgungsträgerdatenbank	Beurteilung der Werthaltigkeit von Lebensversicherungen, die der Kreditbesicherung dienen.	✓	
Mitversicherungsverrechnung	Verrechnung zwischen Mitversicherern	✓	

Datenaustauschplattform	Plattform zum verschlüsselten Datenaustausch	✓	
Schlichtung Krankenversicherung	Koordinierung von Schlichtungsfällen aus der Direktverrechnung		✓
Zentrales Informationssystem der österreichischen Versicherungswirtschaft in der Lebensversicherung	Prüfung von Versicherungsrisiken im Antragsfall		✓
Bonus Malus Auskunft	Prämieneinstufung in der KFZ/HP-Versicherung		✓
Kraftfahrzeug-Zulassungsevidenz	Abwicklung von KFZ-Zulassungen		✓

Die Versicherer informieren in ihrer *Datenschutzinformation* über jene beim VVO zentral betriebenen Systeme, an denen sie teilnehmen und verweisen hinsichtlich ausführlicher Information zu diesen Systemen auf die Homepage des VVO.

4.2.1. LET-Tilgungsträgerdatenbank

Die LET-Tilgungsträgerdatenbank ist ein System, das der VVO betreibt und welches in § 39 BWG und dem Rundschreiben der FMA „Mindeststandards zum Risikomanagement und zur Vergabe von Fremdwährungskrediten und Krediten mit Tilgungsträgern“ (FMA-FXTT-MS; konkret: 18a) seinen Ursprung hat. Es dient dem automatisierten Datenaustausch zwischen Versicherungsunternehmen und Kreditinstituten. Versicherungsunternehmen stellen den Kreditinstituten jene Daten automatisiert zur Verfügung, welche diese zur Beurteilung des Bestehens und der Werthaltigkeit von Tilgungsträgern bzw. Polizzen, die der Kreditbesicherung dienen, benötigen. Jedes teilnehmende Versicherungsunternehmen meldet Lebensversicherungsverträge ein, die zur Kreditbesicherung verwendet werden; berechtigte Kreditinstitute haben Zugriff auf jene Polizzen, die zur Absicherung der von ihnen vergebenen Kredite dienen. Durch die Automatisierung des Datenaustausches wird der Aufwand für den Abgleich und die Überprüfung der Verträge wesentlich reduziert.

Der VVO betreibt dieses System im Auftrag seiner Mitgliedsunternehmen, verfolgt damit keine eigenen Zwecke und fungiert somit als datenschutzrechtlicher Auftragsverarbeiter gemäß Art. 4 Z 8 DSGVO. Auftragsverarbeiterverträge gemäß Art. 28 Abs. 3 DSGVO wurden mit jedem teilnehmenden Versicherungsunternehmen abgeschlossen.

4.2.2. Mitversicherungsverrechnung

Der Datenaustausch zwischen den Versicherungsunternehmen im Rahmen der Mitversicherungs-verrechnung erfolgt über ein System, das beim VVO eingerichtet ist. Die teilnehmenden Unternehmen tauschen standardisierte Prämien- und *Schadendaten* aus, die auf bilateralem Wege für den Saldoab- und -ausgleich im Rahmen einer *Mitversicherung* notwendig sind. Bei jedem Unternehmen wird für eine abgegebene Prämien- oder Schadenverrechnung bzw. -anmeldung ein Datensatz erstellt. Die Datensätze einer Abrechnungsperiode werden an den VVO übermittelt und dort eingelesen, geprüft und nach den abgebenden Unternehmen sortiert an das jeweils übernehmende Unternehmen übermittelt.

Der VVO betreibt dieses System im Auftrag seiner Mitgliedsunternehmen. Diese verwirklichen durch dieses System eine Risikomanagementmaßnahme im Sinne des § 110 VAG. Der VVO verfolgt damit keine

eigenen Zwecke und fungiert somit als datenschutzrechtlicher Auftragsverarbeiter gemäß Art. 4 Z 8 DSGVO. Auftragsverarbeiterverträge gemäß Art. 28 Abs. 3 DSGVO wurden mit jedem teilnehmenden Versicherungsunternehmen abgeschlossen.

4.2.3. Datenaustauschplattform – FTAPI

FTAPI ist ein Produkt zum sicheren und verschlüsselten Empfang und Versand von Dokumenten. Der VVO stellt die Software FTAPI SecuTransfer als gehostete Software in seinem Rechenzentrum zur Verfügung, übernimmt die Wartung und Pflege der Software sowie den Support der Benutzer. Diese Plattform kann von den Versicherungsunternehmen sowie deren Partnern (z.B. Gutachter) zum sicheren Datenaustausch genutzt werden.

Die Bereitstellung der Software durch den VVO erfolgt im Auftrag seiner Mitgliedsunternehmen. Der VVO fungiert als datenschutzrechtlicher Auftragsverarbeiter gemäß Art. 4 Z 8 DSGVO; Auftragsverarbeiterverträge gemäß Art. 28 Abs. 3 DSGVO wurden mit jedem teilnehmenden Versicherungsunternehmen abgeschlossen. Bei Benutzung von FTAPI seitens des VVO für eigene Zwecke ist dieser insoweit selbst Verantwortlicher.

4.2.4. Schlichtung Krankenversicherung

Zwischen privaten Krankenversicherungsunternehmen und deren Vertragspartnern, das sind Krankenanstaltenträger und Ärztekammern, bestehen Vereinbarungen über die Einrichtung von Schlichtungsstellen. Die Schlichtungsstellen sind laut Schlichtungsordnungen zur Verhandlung und Entscheidung über Meinungsverschiedenheiten zuständig. Grundlage hierfür sind Direktverrechnungsverträge zwischen den privaten Krankenversicherungsunternehmen und deren Vertragspartnern und das vom Gesetzgeber anerkannte Konzept der Schlichtung (siehe § 11c VersVG). Der VVO koordiniert auf Grundlage und in Anwendung der Schlichtungsordnungen die Verhandlungen. In diesem Zusammenhang erhält der VVO Unterlagen, welche personenbezogene Daten enthalten.

Der VVO handelt dabei im Auftrag der Versicherungen und fungiert als datenschutzrechtlicher Auftragsverarbeiter gemäß Art. 4 Z 8 DSGVO; Auftragsverarbeiterverträge gemäß Art. 28 Abs. 3 DSGVO wurden mit den privaten Krankenversicherungsunternehmen abgeschlossen.
Die Versicherungsunternehmen verstehen sich in ihrem Wirken in der Schlichtungsstelle als gemeinsam Verantwortliche im Sinne des Art. 26 DSGVO. Zwar legen sie einander weder personenbezogene Daten offen, noch tauschen sie diese untereinander aus oder verarbeiten sie gemeinsam. Jedoch stellen die Versicherungsunternehmen dem Entscheidungsgremium der Schlichtungsstelle bedarfsbezogen ihre Mitarbeiter als unabhängige Fachexperten zur Verfügung. Zur Sicherstellung, dass damit keine Verarbeitung oder Kenntniserlangung von personenbezogenen Daten des Schlichtungsfalls durch jenes Versicherungsunternehmen bewirkt wird, welches die Mitarbeiter zur Verfügung stellt, haben die privaten Krankenversicherungsunternehmen eine Vereinbarung über eine gemeinsame Datenverarbeitung nach Art. 26 DSGVO abgeschlossen.

4.2.5. Zentrales Informationssystem der österreichischen Versicherungswirtschaft in der Lebensversicherung

Die privaten Versicherungsunternehmen Österreichs betreiben beim VVO ein Zentrales Informationssystem ("ZIS") im Bereich der Lebensversicherung. Das ZIS dient dem Schutz der Versichertengemeinschaft vor Versicherungsmissbrauch und der Wahrung der Prämienäquivalenz. Wird ein Versicherungsantrag abgelehnt, unter erschwerten Bedingungen angenommen, wird ein *Versicherungsvertrag* wegen vorvertraglicher Anzeigepflichtverletzung beendet oder wird eine Berufsunfähigkeitsversicherung abgeschlossen

(versicherte Jahresrente > EUR 9.000), so kann die *versicherte* / zu versichernde *Person* ab unterfertigter Antragstellung im System erfasst werden. Ein bestehender Systemeintrag kann von den teilnehmenden Versicherungsunternehmen abgefragt werden.

Das ZIS wird beim VVO betrieben, der im Auftrag der Versicherungen handelt. Diese verwirklichen durch dieses System eine Risikomanagementmaßnahme im Sinne des § 110 VAG. Der VVO verfolgt keine eigenen Zwecke und handelt somit als datenschutzrechtlicher Auftragsverarbeiter gemäß Art. 4 Z 8 DSGVO. Auftragsverarbeiterverträge gemäß Art. 28 Abs. 3 DSGVO wurden mit den teilnehmenden Versicherungsunternehmen abgeschlossen.
Zur gemeinschaftlichen Festlegung der datenschutzrechtlichen Zwecke und Mittel bei der Teilnahme an diesem Informationssystem haben die teilnehmenden Versicherungsunternehmen eine Vereinbarung über eine gemeinsame Datenverarbeitung nach Art. 26 DSGVO abgeschlossen.

4.2.6. Bonus/Malus-Auskunftssystem

Beim VVO wird die Datenaustauschplattform „Bonus/Malus-Auskunftssystem“ betrieben. Zweck ist die Abrufmöglichkeit der Einstufung innerhalb des Bonus/Malus Systems für Kfz-Haftpflichtversicherungsverträge. Daten zur Prämienstufe aus Kfz-Haftpflichtversicherungsverträgen werden von Kfz-Versicherern in die Plattform eingemeldet, wenn die Versicherung ohne Nachfolgevertrag beendet und auf den *Versicherungsvertrag* das Bonus/Malus System angewendet wurde. Die Daten zur Prämienstufe können vom Nachfolgeversicherer abgerufen und der Einstufung im Bonus/Malus System zugrunde gelegt werden.

Die Bereitstellung der Datenaustauschplattform durch den VVO erfolgt im Auftrag seiner Mitgliedsunternehmen, die die Kfz-Haftpflichtversicherung betreiben. Diese verwirklichen durch dieses System eine Risikomanagementmaßnahme im Sinne des § 110 VAG. Der VVO verfolgt damit keine eigenen Zwecke und fungiert somit als datenschutzrechtlicher Auftragsverarbeiter gemäß Art. 4 Z 8 DSGVO; Auftragsverarbeiterverträge gemäß Art. 28 Abs. 3 DSGVO wurden mit den teilnehmenden Versicherungsunternehmen abgeschlossen.
Zur gemeinschaftlichen Festlegung der datenschutzrechtlichen Zwecke und Mittel bei der Teilnahme an diesem System haben die teilnehmenden Versicherungsunternehmen eine Vereinbarung über eine gemeinsame Datenverarbeitung nach Art. 26 DSGVO abgeschlossen.

4.2.7. Kraftfahrzeug-Zulassungsevidenz

Der VVO betreibt zur einheitlichen Durchführung aller Fahrzeugzulassungen in Österreich das Informationssystem ”Kraftfahrzeug-Zulassungsevidenz” für beliehene Versicherungsunternehmen, einschließlich automationsunterstützt erstellter und archivierter Textdokumente.
Gemäß § 47 (4a) KFG hat die Gemeinschaftseinrichtung der zum Betrieb der Kraftfahrzeug-Haftpflichtversicherung berechtigten Versicherer, die gemäß § 40b Abs. 6 Z 2 KFG erfassten und übermittelten Daten in einer zentralen Zulassungsevidenz zu erfassen und zu speichern.
Die berechtigten Versicherer wurden vom zuständigen Landeshauptmann gemäß § 40a Abs. 4 KFG im Rahmen des Betriebs einer Kraftfahrzeug-Haftpflichtversicherung mit Bescheid zur Errichtung von Zulassungsstellen und mit der Durchführung der KFZ-Zulassungen ermächtigt.
Das Informationssystem wurde als ein Informationsverbundsystem eingerichtet, als solches beim österreichischen Datenverarbeitungsregister registriert, und es wird gemeinsam von den am Informationssystem teilnehmenden Versicherungsunternehmen iSd Art. 26 DSGVO betrieben. Als Gemeinschaftseinrichtung und Auftragsverarbeiter des Informationssystems ist aufgrund einer gremialen Entscheidung der VVO bestellt.

Auftragsverarbeiterverträge gemäß Art. 28 Abs. 3 DSGVO wurden mit den teilnehmenden Versicherungsunternehmen abgeschlossen.
Zur gemeinschaftlichen Festlegung der datenschutzrechtlichen Zwecke und Mittel bei der Teilnahme an diesem Informationssystem haben die teilnehmenden Versicherungsunternehmen eine Vereinbarung über eine gemeinsame Datenverarbeitung nach Art. 26 DSGVO abgeschlossen.

4.3. Selbstständige Versicherungsvermittler

Versicherungsvermittler sind in ihrer berufsrechtlichen Grundbetrachtung datenschutzrechtlich Verantwortliche, da sie weisungsungebundene Bewertungen und Interessenabwägungen vornehmen und hierbei als Verantwortliche die Zwecke und Mittel ihrer Datenverarbeitungen selbst bestimmen. Zusätzlich können sie jedoch auch als datenschutzrechtlicher Auftragsverarbeiter des Versicherers agieren, indem sie für den Versicherer auftragsbezogene Geschäftstätigkeiten und die damit verbundenen datenschutzrechtlichen Datenverarbeitungen als dessen Auftragsverarbeiter vornehmen.

Versicherung und *Versicherungsvermittler* schließen– sofern erforderlich - die entsprechenden datenschutzrechtlichen Vereinbarungen. In jedem Fall werden zwischen den Vertragsparteien die nach Maßgabe der jeweiligen Verarbe**i**tungszwecke und der dabei zum Einsatz gelangenden technischen Mittel, die wechselseitigen datenschutzrechtlichen Verantwortlichkeiten und Zuständigkeiten zur Sicherstellung der Betroffenenrechte festgelegt. Versicherung und *Versicherungsvermittler* tragen innerhalb ihrer Verantwortungsbereiche jederzeit für eine rechtmäßige und dem Stand der Technik entsprechende und vertrauliche, Verarbeitung personenbezogener Daten Sorge.

Beispielanwendungsfall:
Stellt der Versicherer dem *Versicherungsvermittler* ein IT-System (z.B. Portal) zur Verfügung, in dem er alleine über Zwecke, Funktionen, Zugriffe und wesentliche Elemente der einzusetzenden Mittel entscheidet, ist der Versicherer datenschutzrechtlich Verantwortlicher für dieses Portal.
Der Vermittler übt seine Tätigkeit im Umfang seiner Gewerbeberechtigung als selbständiger *Versicherungsvermittler* aus. Im Rahmen dieser Tätigkeit verarbeitet der Vermittler personenbezogene
Daten als Verantwortlicher.

4.4. Sonstige Empfänger

Im Rahmen des Versicherungsbetriebs ist es erforderlich, dass Versicherer personenbezogene Daten an verschiedene externe Empfänger übermitteln. Eine Datenübermittlung erfolgt selbstverständlich nur dann, wenn dies zur Vertragserfüllung notwendig ist oder eine rechtliche Verpflichtung bzw. Ermächtigung vorliegt, dies zur Wahrung eines überwiegenden berechtigten Interesses des Versicherers oder eines Dritten erforderlich ist oder die Einwilligung des Betroffenen dazu vorliegt. Die Empfänger agieren bei ihrer Tätigkeit und der damit verbundenen Datenverarbeitung entweder als eigenständig Verantwortliche (d.h. sie unterliegen selbst den Verpflichtungen der DSGVO), als Auftragsverarbeiter für Versicherer (auf Basis einer Auftragsverarbeitervereinbarung nach Art. 28 DSGVO) oder als gemeinsame Verantwortliche (auf Basis einer Vereinbarung nach Art. 26 DSGVO, siehe zu den datenschutzrechtlichen Rollenkonzepten in der Versicherungswirtschaft: Kapitel 4.2).

Folgende externe Empfänger sind typischerweise als selbstständig **Verantwortliche** tätig:

Empfänger	**Tätigkeit / Zweck der Übermittlung**

Rückversicherer	*Rückversicherung* der vom Versicherer übernommenen Erstrisiken (Risikobeurteilung und Prüfung von rückversicherten Schadenfällen)
Mitversicherer	Risikoteilung durch teilweise Übernahme von großen Erstrisiken (Risikobeurteilung und Abwicklung von Schadenfällen, an denen der Mitversicherer beteiligt ist)
Abtretungs-, Pfand- und Vinkulargläubiger	Sicherstellung von Rechten an *Versicherungsverträgen* auf Basis vertraglicher Vereinbarungen zwischen Gläubiger (z.B. Leasinggeber, Kreditgeber, Hypothekargläubiger) und *Versicherungsnehmer*
Sachverständige, Gutachter	Erstellung von Sachverständigengutachten (v.a. in Schadenfällen)
Professionisten, Werkstätten	Durchführung von Schadenbehebungen (z.B. Reparaturen)
Gesundheitsdienstleister (z.B. Ärzte, Krankenanstalten, Reha-Zentren, Apotheken)	Erfüllung des *Versicherungsvertrages* (z.B. Direktverrechnung von Leistungen im Rahmen der Krankenversicherung)
Rechtsanwälte	Geltendmachung oder Abwehr von Rechtsansprüchen Erfüllung des *Versicherungsvertrages*
Detektei	Geltendmachung oder Abwehr von Rechtsansprüchen
Banken, Kreditinstitute	Abwicklung von Zahlungsverkehr (z.B. Einzug von Versicherungsprämien)
Inkassobüros	Geltendmachung von Forderungen
Notare, Gerichtskommissäre	Durchführung von Verlassenschaftsverfahren
Kreditauskunftei	Bonitätsprüfung und Bonitätsauskünfte
Insolvenzverwalter	Durchführung von Insolvenzverfahren
Wirtschaftsprüfungs- und Steuerberatungsunternehmen	Prüfung des Jahresabschlusses
Einrichtungen der Streitbeilegung (Interessenvertretungen, Schlichtungsstellen)	Außergerichtliche Regulierung von strittigen Ansprüchen
Gerichte, Staatsanwaltschaft, Finanzbehörden, Aufsichtsbehörden	Erfüllung von gesetzlichen Verpflichtungen, denen Versicherer unterliegen
Konzernverbundene Unternehmen	Rechtliche Anforderungen, Konzernsteuerung, Marketing
Kooperationspartner	Marketing
Berufsgruppenvertretungen	Übermittlung von Pflichtversicherungsbestätigungen
Schadenregulierungsbeauftragte	Regulierung von KFZ-Haftpflicht – Schäden gemäß §100 VAG
Telekommunikationsunternehmen	Erbringung von Telekommunikationsdienstleistungen nach TKG

Folgende externe Empfänger sind typischerweise als **Auftragsverarbeiter** tätig:

Empfänger	**Tätigkeit / Zweck der Übermittlung**
IT-Dienstleister	Betrieb und Wartung von Rechenzentren und IT-Systemen, Entwicklung und Betreuung von Software inkl. Audio- und Videokommunikationssoftware
Scan- und Druckdienstleister	Digitalisierung von Dokumenten, Druck und Kuvertierung von Poststücken
Aktenvernichter	Fachgerechte Entsorgung von Papierakten und Datenträgern

Call Center, Customer Care Service	Betreuung von Anfragen über unterschiedliche Kommunikationskanäle (z.B. Telefon, E-Mail, Chat)
Schadenregulierer	Betreuung und Abwicklung von Schadenfällen
Assistance Dienstleister	Vermittlung von Assistance Dienstleistungen (z.B. Organisation eines Schlüsseldienstes)
Werbe- /Marketingagenturen	Durchführung von Werbekampagnen (z.B. Versand von E-Mails) und Gewinnspielen
Marktforschungsinstitute	Durchführung von Meinungsumfragen und Marktanalysen
Externer Underwriter	Zeichnung von Risiken

Bei dieser Darstellung handelt es sich um eine typisierende Betrachtung; abhängig von den tatsächlichen Verhältnissen und den vertraglichen Grundlagen können die genannten Empfänger in Einzelfällen auch in einer anderen datenschutzrechtlichen Rolle tätig sein.

4.5. Übermittlungen personenbezogener Daten in Drittländer oder an internationale Organisationen

Versicherer bieten ihren *Kunden* einen umfassenden Versicherungsschutz, der im Interesse der *Kunden* abhängig vom jeweiligen Produkt/Tarif häufig nicht an den österreichischen oder europäischen Grenzen endet. Vor allem aufgrund dieser Tatsache ist es im Rahmen der Vertragsbeziehung als auch zur Geltendmachung, Ausübung und Abwehr von etwaigen Rechtsansprüchen in Einzelfällen erforderlich, dass personenbezogene Daten im erforderlichen Ausmaß an Empfänger in *Drittländern* – sohin außerhalb des EU/EWR-Raumes – übermittelt werden. Gelegentlich ist somit eine Übermittlung personenbezogener Daten in *Drittländer* im Zusammenhang mit Leistungspflichten in einem Schadens- oder Leistungsfall erforderlich (z.B. Wanderunfall oder KFZ-Unfall außerhalb EU/EWR). Des Weiteren können Übermittlungen von personenbezogenen Daten zur Vertragserfüllung auch an Empfänger in *Drittländer* beispielsweise im Rahmen von *Rück*- oder *Mitversicherung* erforderlich sein.

Zum Zeitpunkt der Erstellung dieses Branchenstandards sind diverse Rechtsfragen zur Übermittlung personenbezogener Daten an Empfänger in *Drittländern* offen und der diesbezügliche Rechtsvollzug ist im Fluss. Dennoch bilden solche Datenübermittlungen in der aktuellen Praxis oftmals eine unabdingbare Notwendigkeit für den Versicherungsbereich, so etwa bei Datenübermittlungen an nicht im EWR ansässige Mit- und Rückversicherer. Im Sinne größtmöglicher Rechtssicherheit angesichts des noch in Klärung befindlichen Rechtsrahmens wird diesbezüglich im Rahmen dieses Branchenstandards festgehalten, dass, soweit eine Datenübermittlung nicht aufgrund eines Angemessenheitsbeschlusses (Art. 45 DSGVO), oder aufgrund von geeigneten Garantien (wie z.B. Standarddatenschutzklauseln) iSd Art. 46 DSGVO und zugehörigen Maßnahmen ("supplementary measures") oder verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules einer Unternehmensgruppe) als Rechtsgrundlage für die Übermittlung erfolgen kann, die Versicherer im zur Erledigung eines Geschäftsfalls erforderlichen Einzelfall personenbezogene Daten an Empfänger in *Drittländern* gemäß Art. 49 DSGVO insbesondere zum Zwecke der Erfüllung des jeweiligen *Versicherungsvertrages* oder zur Durchführung vorvertraglicher Maßnahmen auf Antrag der betroffenen Person (lit b), zum Abschluss oder zur Erfüllung eines *Versicherungsvertrages* im Interesse der betroffenen Person (lit c), und auch zur geschäftsfallbezogenen Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (lit e) übermitteln. Derartige Geschäftsfälle werden entsprechend der technischen Möglichkeiten vermerkt. Hiervon unberührt bleibt das Verständnis, dass die Rechtsgrundlagen des Art. 49 DSGVO als einzelfallbezogene Ausnahmetatbestände zu verstehen sind, welche insbesondere zur Anwendung gelangen, wenn nicht mit Standarddatenschutzklauseln das Auslangen gefunden werden kann oder diese nicht zur Anwendung gebracht werden können.

5. Datenverarbeitung

5.1. Kategorien der Verarbeitungszwecke und Rechtsgrundlagen

Das Angebot und die Leistungen von Versicherern sind in Österreich durch (aufsichts-) rechtliche Bestimmungen, wie insbesondere dem VAG und dem VersVG, sowie den Vorgaben der Finanzmarktaufsichtsbehörde (FMA) reguliert.
Im Rahmen ihrer Kerntätigkeit, also der Anbahnung, dem Abschluss und der Erfüllung von *Versicherungsverträgen*, verarbeiten Versicherer personenbezogene Daten, insbesondere für die in der untenstehenden Tabelle dargestellten Zwecke.

Vor der Verarbeitung der Daten prüft der Versicherer im Detail, welche Daten er für den konkreten Zweck benötigt und auf welcher Rechtsgrundlage er eine Datenverarbeitung durchführt. Jedenfalls ist die Verarbeitung von personenbezogenen Daten für den Abschluss und die Erfüllung des jeweiligen *Versicherungsvertrages* erforderlich. Werden die notwendigen personenbezogenen Daten nicht angegeben (durch die betroffene Person selbst oder z.B. durch eine von dieser ermächtigten anderen Person), kann kein *Versicherungsvertrag* abgeschlossen bzw. erfüllt werden. Die Notwendigkeit zur Verarbeitung begründet die Vertragserfüllung des Art. 6 Abs. 1 lit b DSGVO, die Erfüllung einer rechtlichen Verpflichtung im Sinne des Art. 6 Abs. 1 lit c oder berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit f DSGVO, abhängig von der Rolle der betroffenen Person im Versicherungsverhältnis (*Versicherungsnehmer, versicherte Person, Bezugsberechtigter, Geschädigter, Prämienzahler*,…). Für die Erfüllung eines *Versicherungsvertrages*, beispielsweise in der Kranken-, Unfall-, Lebens-, sowie der Rechtsschutzversicherung, kann auch die Verarbeitung von Gesundheitsdaten erforderlich sein. Diese Verarbeitung stützt sich regelmäßig auf die anwendbaren gesetzlichen Sonderbestimmungen (insb. §§ 11a bis 11d VersVG) oder auf Art. 9 Abs. 2 lit f DSGVO. In darüber hinaus gehenden Fällen wird eine Einwilligung eingeholt.

Bei der Verarbeitung von Gesundheitsdaten sind zu den allgemeinen Verarbeitungsvoraussetzungen des Art. 6 Abs. 1 DSGVO auch die in Art. 9 Abs. 2 DSGVO festgelegten Vorrausetzungen zu beachten.
Insofern prüft der Versicherer im Umfang der für eine Antrags- oder Leistungsfallprüfung erforderlichen Gesundheitsdatenverarbeitung stets auch die Voraussetzungen des Art. 9 Abs. 2 DSGVO. Hierbei ist von der Einholung von Einwilligungserklärungen als Rechtsgrundlage nur im gebotenen Maß Gebrauch zu machen. Dies erfolgt insbesondere dann, wenn kein anderer Ausnahmetatbestand die Verarbeitung rechtfertigt. Als im Regelfall anwendbare Rechtfertigungsgründe der Verarbeitung personenbezogener Gesundheitsdaten stellen sich § 11a VersVG sowie die konkretisierenden Bestimmungen dieses Branchenstandards zur voll- und teilautomatisierten Erhebung und Verarbeitung personenbezogener Gesundheitsdaten zur Antrags- und Leistungsfallprüfung, § 11b VersVG zur Verarbeitung und Übermittlung personenbezogener Gesundheitsdaten in der Direktverrechnung und § 11c VersVG zur geschäftsfallbezogenen Datenübermittlung an Mit- und Rückversicherer, zur Behandlung in der Schlichtungsstelle sowie zur geschäftsfallbezogenen Datenübermittlung an Sachverständige dar.

Die Verarbeitung in der Versicherungsbranche stützt sich in der Regel auf die unten aufgelisteten Rechtsgrundlagen und Zwecke. Die aufgelistete Rechtsgrundlagenzuweisung hat nur typisierenden Charakter und bietet insofern eine Rechtsgrundlagenzuweisung für den Regelfall. Ungeachtet dessen ist stets eine einzelfallbezogene Rechtsgrundlagenprüfung vorzunehmen und diese kann ergeben, dass die Verarbeitung der Daten auch aufgrund anderer, von der typisierenden Rechtsgrundlagenzuweisung abweichender Rechtgrundlagen erfolgen kann.

Rechtsgrundlage	Zweck
Vertragserfüllung oder Durchführung vorvertraglicher Maßnahmen auf Anfrage der betroffenen Person (Art. 6 Abs. 1 lit b DSGVO) & Gesetzliche Sonderbestimmungen für die Verarbeitung von Gesundheitsdaten (Art. 9 Abs. 2 lit g, h und Abs. 4 DSGVO: z.B. § 11a bis 11d VersVG)	✓ Anbahnung der Geschäftsbeziehung (wie z.B. Beratung, Offert, Anbot, Vorschlag), Antragserstellung, Vertragserstellung (Versicherungspolizze) und Vertragsänderungen. Dies beinhaltet die Einschätzung des zu übernehmenden Risikos zur Beurteilung, ob und zu welchen Bedingungen der *Versicherungsvertrag* abgeschlossen bzw. eine Vertragsänderung durchgeführt werden kann. ✓ Durchführung, Erfüllung, Verwaltung (inkl. Prämieninkasso) und Beendigung des *Versicherungsvertrages* wie auch Rechnungslegung, laufende Kundenbetreuung und –beauskunftung sowie Verwaltung von *Stammdaten*- und *Vertragsdaten*änderungen. ✓ Erfassung von Informationen zur Schadenbearbeitung, Ermittlung und Prüfung des Leistungsanspruchs sowie Leistungsabwicklung. Dies inkludiert in der Krankenversicherung auch die eingerichtete Schlichtungsstelle zu Leistungsfällen zwischen Versicherungswirtschaft und verschiedenen Krankenanstaltenträgern und die gesetzlich eingerichtete Direktverrechnung (§§ 11a bis 11d VersVG). Hinweis: Die Vertragserfüllung (Art. 6 Abs. 1 lit b DSGVO) stellt bei *versicherten Personen*, *Bezugsberechtigten*, Gläubigern und beim *Geschädigten* ein berechtigtes Interesse (Art. 6 Abs. 1 lit f DSGVO) dar.
Erfüllung rechtlicher Verpflichtungen (Art. 6 Abs. 1 lit c DSGVO) & Gesetzliche Sonderbestimmungen für die Verarbeitung von Gesundheitsdaten (Art. 9 Abs. 2 lit g, h und Abs. 4 DSGVO)	✓ Der Versicherer hat gesetzliche Verpflichtungen wie aufsichtsrechtliche Vorgaben, Beratungs- und Informationspflichten (z.B. Belehrung über Rücktrittsrechte) sowie steuer- oder unternehmensrechtliche Vorgaben. Damit der Versicherer diese erfüllen kann, verarbeitet er personenbezogene Daten ausschließlich in dem vom jeweiligen Gesetz erforderlichen Umfang. ✓ Administration des KFZ-Zulassungsgeschäfts als beliehener Versicherer iSd KFG Zulassungsstellenverordnung wie z.B. für die An- und Abmeldung eines KFZ ✓ Einhaltung des ordnungsgemäßen Geschäftsbetriebs. Darunter ist die Konformität mit nationalen gesetzlichen und anderen Anforderungen, wie etwa VAG, VersVG, FM-GwG, DSG, UGB, BWG, AktG, BAO, EStG, ASVG, VersStG, Sanktionsprüfungen sowie EU-rechtlichen Vorgaben (z.B. Solvency II, DSGVO) und auch Aufzeichnungs-/ Berichtsverpflichtungen, interne Revisionsmaßnahmen, Konformität mit Überprüfungen durch Behörden, Verwaltung interner Beschwerden/Ansprüche, zu verstehen. ✓ Die Gewährleistung der IT Sicherheit und des IT Betriebs, Durchführung von Belastungstests, Entwicklung von neuen sowie Adaptierung der bestehenden Produkte und Systeme, Migration von Daten vor allem zur Sicherstellung der Funktions- und Leistungsfähigkeit der Systeme und damit im weiteren Sinn auch der verarbeiteten Daten (Art. 32 DSGVO, aufsichtsrechtliche Vorgaben). Dabei werden die angegebenen personenbezogenen Daten vorwiegend für

	Tests verwendet, wo dies nicht mit vertretbarem wirtschaftlichem Aufwand auf Basis von anonymen Daten erfolgen kann.
Berechtigte Interessen (Art. 6 Abs. 1 lit f DSGVO) inklusive Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 9 Abs. 2 lit f DSGVO)	✓ Erstellung von Analysen und Statistiken (z.B. zur Entwicklung neuer Produkte und Services, Kundenbetreuung, Offert- und Antragsbearbeitung, Vertragsverwaltung, Leistungserbringung, Schadenabwicklung und Risikominimierung). ✓ Laufende Verbesserung der Geschäftsprozesse (z.B. Antragsbearbeitung, Schadenbearbeitung) durch deren quantitative und qualitative Analyse (wie z.B. Erreichbarkeit, Reaktionszeit, Bearbeitungszeit) zur Optimierung der Beratungs- und Betreuungsqualität und Sicherstellung der operativen Geschäftsfallbearbeitung. ✓ Einholen von Bonitätsauskünften, insbesondere bei hohen Risiken und bei Ermittlungen im Schadenfall ✓ Verhinderung und Aufklärung von Straftaten. Dazu nutzt der Versicherer insbesondere Datenanalysen, um Hinweise zu erkennen, die auf Versicherungsmissbrauch hindeuten. ✓ Verhinderung, dass *Versicherungsnehmer* zu Bedingungen versichert werden oder Leistungen erhalten, die nicht im Einklang mit dem *Risikoausgleich* der Versichertengemeinschaft stehen. Zur Erfüllung dieser Zwecke tauscht der Versicherer z.B. in der Lebensversicherung personenbezogene Daten mit dem Zentralen Informationssystem der Versicherungswirtschaft (ZIS) aus. ✓ Im Rahmen der Kfz-Haftpflichtversicherung erhält der Versicherer Informationen über den Schadenverlauf vom Vorversicherer, um die korrekte Einstufung in das Bonus-Malus System zu ermöglichen und um die Prämie nach Maßgabe des Schadenverlaufes zu berechnen. ✓ Der Versicherer muss in unterschiedlichen Anlassfällen die dafür erforderlichen Daten – insbesondere die vorhandenen Daten zum Vertrag, Leistungen und zugehörige Beratung sowie Erkenntnisse aus der laufenden Kundenbeziehung inkl. Gesundheitsdaten – zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (wie z.B. gerichtlichen, außergerichtlichen oder verwaltungsbehördlichen Verfahren) verarbeiten
Einwilligung (Art. 6 Abs. 1 lit a, Art. 9 Abs. 2 lit a DSGVO)	✓ Versicherer holen eine Einwilligung nach der DSGVO nur dann ein, wenn keine andere Rechtsgrundlage besteht. ✓ Eine dokumentierte Einwilligung wird z.B. auch vor einer Aufzeichnung bei Telefonaten und Videoberatungen eingeholt sowie für bestimmte Marketingmaßnahmen (siehe 5.2 Marketingmaßnahmen)
Gesetzliche Einwilligung gem. Art. 9 Abs. 2 lit g DSGVO iVm § 11a VersVG	✓ Freiwillige und jederzeit widerrufbare Einwilligungen benötigt der Versicherer vor allem bei Ermittlung der Gesundheitsdaten bei Dritten wie z.B. Ärzten, Krankenanstalten, Sozialversicherungsträger, Therapeuten und Gutachter gemäß §§ 11a bis 11d VersVG in einem für den Vertragsabschluss bzw. die Vertragsänderung sowie die Leistungserbringung im gesetzlich definierten Umfang.

Die personenbezogenen Daten werden grundsätzlich im Rahmen der den betroffenen Personen bekannten und über die Datenschutzhinweise nach Art. 13 bzw. 14 DSGVO kommunizierten Zweckbestimmungen verarbeitet. Eine Änderung oder Erweiterung der Zweckbestimmung erfolgt nur, wenn sie rechtlich zulässig ist und die betroffenen Personen darüber informiert wurden (siehe Kapitel 6) oder wenn die betroffenen Personen gesondert eingewilligt haben.

5.2. Marketingmaßnahmen

Versicherer haben teilweise produkt- oder servicespezifische Marketingmaßnahmen etabliert, die zu einer Kontaktaufnahme mit *Kunden* führen. Dabei werden bestimmte Kriterien wie z.B. bestehende Versicherungstarife, Alter, demographische Aspekte zur Vorselektion der entsprechenden *Kunden* herangezogen. Sofern dabei persönliche Aspekte berücksichtigt werden sowie Rechtswirkungen damit verknüpft sind, sind die Bestimmungen des Art. 22 DSGVO einzuhalten. Die folgenden Maßnahmen stützt der Versicherer dabei entweder auf eine Einwilligung (Art. 6 Abs. 1 lit a DSGVO) oder auf berechtigte Interessen (Art. 6 Abs. 1 lit f DSGVO), je nachdem welche personenbezogenen Daten und/oder welcher Kommunikationskanal dafür verwendet werden soll. Davon unberührt bleiben die Bestimmungen des TKG betreffend die Zusendung von elektronischer Post bzw Telefonanrufen. In der nachfolgenden Tabelle finden sich klassische Anwendungsfälle in der Versicherungsbranche unter Berücksichtigung von Kontaktwegen wie z.B. elektronische Kommunikationsmittel, Telefon, Post:

Anwendungsfälle	**Zweck**
Marktforschung	Erhebung bei Marktteilnehmern und – darauf aufbauend – Verbesserung der Prozesse und Produkte/Services.
Werbemaßnahmen z.B. Newsletterversand oder postalischer Versand	Allgemeine und zielgerichtete Informationen zu Services (z.B. Apps, Kundenportalen), Gewinnspielen, Veranstaltungen, Unternehmensinitiativen an bestehende *Kunden* und Interessenten.

Ein Widerspruch im Sinne des Art. 21 Abs. 2 und 3 DSGVO zur Verarbeitung personenbezogener Daten zu Marketingzwecken ist vom Versicherer immer zu berücksichtigen.

5.3. Maßnahmen Kundenbetreuung

Die in diesem Punkt beschriebenen Datenverarbeitungen stellen keine Marketingmaßnahmen dar, sondern leiten sich aus der besonderen Vertragssituation im Versicherungsbereich und der im Folgenden beschriebenen Erwartungshaltung der *Kunden* ab und liegen im berechtigten Interesse (Art. 6 Abs. 1 lit f DSGVO) des Versicherers. Das Widerspruchsrecht des Art. 21 Abs. 2 und 3 DSGVO bleibt davon unberührt.

5.3.1. Evaluierung der Risikosituation und Beratung

Das Versicherungsverhältnis ist von einer besonderen Vertrauenskomponente, einem Treueverhältnis und Beratungsintensität geprägt. Aufgrund der Komplexität und der langen Laufzeit der Produkte werden an Versicherer hohe Beratungs- und Aufklärungsanforderungen gegenüber ihren *Kunden* gestellt. Dies dient dazu, den Versicherungsschutz an die aktuelle Risikosituation anzupassen und um eventuelle Deckungslücken aufzeigen bzw. schließen zu können. Die Versicherer unterliegen entsprechend der aufsichtsrechtlichen Vorgaben einer Beratungspflicht (§§ 132, 135a Abs. 3 VAG). Die Risikosituation der *Kunden* kann während dem aufrechten *Versicherungsvertrag* einem Wandel unterliegen. Deshalb ist es auch während des aufrechten Vertrages zweckmäßig den *Kunden* zu kontaktieren und die Risikosituation durch Erhebung der Wünsche und Bedürfnisse zu evaluieren, um entsprechend zugeschnittene bzw. angepasste Produkte und Services zu empfehlen. Diese Erwartungshaltung der *Kunden* an die regelmäßige Evaluierung der

Wünsche und Bedürfnisse manifestiert sich auch aus der einschlägigen Rechtsprechung[2] und in der aufsichtsbehördlichen Praxis der Finanzmarktaufsicht[3].
Sofern ein Versicherer, ohne zuvor einen entsprechenden Bedarf erhoben zu haben bzw. ohne vorherige Interessensbekundung eines *Kunden,* Informationen zu einem Versicherungsprodukt an einen *Kunden* versenden möchte, welches einer anderen Versicherungssparte als die bereits bestehenden Versicherungsverträge des *Kunden* zuzuordnen ist und welches offenkundig nicht als Zusatzdeckung oder als erweiterte Risikoabdeckung zu sehen ist, so handelt es sich dabei um eine Marketingmaßnahme. Für diese gelten daher die Ausführungen unter Punkt 5.2. In diesem Sinne kann z.B. ein Angebot zu einer Kfz-Versicherung im Zuge einer Re-Evaluierung einer bestehenden Haushaltsversicherung ohne Interessensbekundung des *Kunden* nur unter Einhaltung der Bestimmungen für Marketingaktivitäten versendet werden.

5.3.2. Zufriedenheitsumfragen zur Verbesserung der Servicequalität

Um eine hohe Servicequalität zu gewährleisten und diese auch stetig zu verbessern, führen Versicherer Zufriedenheitsumfragen bei bestehenden *Kunden* durch. Zufriedenheitsumfragen werden stets durch klar definierte Kriterien ausgelöst (z.B. Kundenkontakt bei Vertragsabschluss/Schaden, sonstige Vertragsverwaltungsmaßnahmen oder kein Kundenkontakt über einen bestimmten Zeitraum) und stellen keine Marketingmaßnahmen im Sinne des §174 TKG dar, weil dies eine Maßnahme im Sinne der aufsichtsrechtlichen Wahrung der Interessen der *Versicherungsnehmer* und sonstigen Anspruchsteller (vergleiche § 267 und § 308 VAG sowie § 74 VersVG) und nicht zuletzt auch eine notwendige Ergänzung des aufsichtsrechtlich geschuldeten funktionierenden Beschwerdemanagements[4] ist. In der Haftpflichtversicherung ist beispielsweise nicht der *Kunde* des Versicherers, sondern ein von diesem geschädigter Dritter der Empfänger der Versicherungsleistung. Dieser Dritte nimmt daher die Rolle des *Kunden* als „Anspruchsteller“ in der Leistungsabwicklung ein. Um auch hier eine ordnungsgemäße Evaluierung der Qualität der Leistungsabwicklung (wie in § 267 VAG gefordert) gewährleisten zu können, führt der Versicherer auch Zufriedenheitsumfragen bei *Geschädigten* durch, jedoch nur in einem engen zeitlichen Kontext zur konkreten Leistungserbringung.

5.4. Umgang mit Gesundheitsdaten, strafrechtlichen Daten und Daten Minderjähriger

5.4.1. Verarbeitung von Gesundheitsdaten

In vielen Fällen müssen Versicherer im Rahmen der (vor-)vertraglichen Versicherungsverhältnisse mit den *Kunden* Gesundheitsdaten verarbeiten, so etwa als Teil der zu einem Schadensfall gemeldeten Schadensdaten; nur in den wenigsten Fällen ist dafür eine gesonderte Einwilligung erforderlich.
Die Verarbeitung von Gesundheitsdaten sowie auch deren Übermittlung an gesetzlich definierte Dritte, wie u.a. Sachverständige, Gesundheitsdienstleister oder (Rück-, Mit-)Versicherer, ist unter den Voraussetzungen der §§ 11a bis 11c VersVG iVm Art. 9 Abs. 2 lit g und h sowie Abs. 4 iVm Art. 6 Abs. 1 DSGVO explizit zulässig. Dies deckt vor allem die notwendige Verarbeitung zur (i) Beurteilung, ob und zu welchen Bedingungen ein *Versicherungsvertrag* abgeschlossen oder geändert wird, (ii) Verwaltung bestehender *Versicherungsverträge* und (iii) Beurteilung und Erfüllung von Ansprüchen aus einem *Versicherungsvertrag*.

[2] siehe OGH 7 Ob 72/11f

[3] siehe etwa Prüfungsschwerpunkte 2020 und 2021 zu Produktentwicklung und Vertrieb

[4] EIOPA-BoS-12/069 DE Leitlinien zur Beschwerdebearbeitung durch Versicherungsunternehmen

Bei der Prüfung und Abwicklung von Regressforderungen oder Ansprüchen *versicherter Personen*, *Geschädigter* in der Haftpflichtversicherung oder *Gegner* in der Rechtsschutzversicherung und bei der Aufdeckung von Versicherungsmissbrauch bildet Art. 9 Abs. 2 lit f DSGVO die Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten (Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen).
Ebenso kann die Verarbeitung von Gesundheitsdaten ohne Einwilligung zum Schutz lebenswichtiger Interessen der betroffenen oder anderer Personen erfolgen, wenn diese aus körperlichen oder rechtlichen Gründen außerstande sind, ihre Einwilligung zu geben (wie etwa bei Assistance-Leistungen (z.B. Notrufdienste) oder weil nach einem Unfall ein Krankentransport für eine bewusstlose Person nötig ist).
In bestimmten Fällen ist eine Einwilligung zur Verarbeitung von Gesundheitsdaten nach Art. 9 DSGVO bzw. § 11a VersVG erforderlich. Das gilt jedenfalls zur Einholung von Gesundheitsdaten bei Dritten (z.B. bei der Einbeziehung von externen Ärzten). Sofern diese nicht erteilt oder widerrufen wird, muss der Betroffene die erforderlichen Informationen selbst beibringen.
Bei der Versicherung von Gesundheitsrisiken werden die Anforderungen des GTelG beachtet. Die Anforderungen des § 6 GTelG werden durch entsprechende technische Maßnahmen (wie etwa Transportverschlüsselung von E-Mails, Verwendung von sicheren Datenaustauschplattformen) sichergestellt.

5.4.2. Verarbeitung strafrechtlicher Daten

Versicherer müssen im Rahmen ihrer Tätigkeiten (z.B. im Falle einer Rechtsschutz- oder Haftpflichtversicherung) teilweise auch personenbezogene Daten über gerichtliche oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, sowie über den Verdacht der Begehung von Straftaten, strafrechtliche Verurteilungen oder vorbeugende Maßnahmen verarbeiten. Die Verarbeitung solcher strafrechtlichen Daten erfolgt ausschließlich im Einklang mit den bzw. auf der Rechtsgrundlage der Bestimmungen des § 4 Abs. 3 Z 1 und 2 DSG iVm Art. 10 DSGVO.[5]

5.4.3. Verarbeitung von Daten Minderjähriger

Versicherer bieten Versicherungsschutz auch für Kinder, unmündige und mündige Minderjährige an. Deren Daten werden bis zur Volljährigkeit idR in der Rolle als *versicherte Person* erfasst, während ein Erziehungsberechtigter als *Versicherungsnehmer* fungiert. In Ausnahmenfällen fungiert der Minderjährige als *Versicherungsnehmer*. Die damit verknüpfte Datenverarbeitung richtet sich nach den bisher dargestellten Grundsätzen und Rechtsgrundlagen, dies jedoch unter besonderer Berücksichtigung des Minderjährigenstatus des *Versicherungsnehmers*.
In Bezug auf Einwilligungen gilt Folgendes:
Sowohl für Kinder als auch unmündige Minderjährige iSd § 21 ABGB können deren gesetzlichen Vertretungsberechtigten (z.B. Erziehungsberechtigte, Obsorgeberechtigte, Pflegschaftsgericht, gesetzlichen Vormunde) eine DSGVO-konforme Einwilligung erteilen. Ab der Vollendung des vierzehnten Lebensjahres ist bei mündigen Minderjährigen eine Einwilligung analog zu § 4 Abs. 4 DSG direkt durch den betroffen mündig Minderjährigen möglich und auch weiterhin durch die gesetzlichen Vertretungsberechtigten. Sofern bereits eine gültige Einwilligung eingeholt wurde, verliert diese ihre Gültigkeit erst durch (i) Widerruf der gesetzlichen Vertretungsberechtigten oder des Betroffenen selbst (ab Vollendung des vierzehnten Lebensjahres) oder (ii) Einholung einer neuen Einwilligung des Betroffenen z.B. bei einer Konvertierung des Vertrags (d.h. Vertragsübernahme durch den nunmehr Volljährigen als neuer *Versicherungsnehmer*). In allen anderen Fällen bleibt die bisher erteilte Einwilligung aufrecht.

[5] Vgl. die erläuternden Erklärungen zum kollektiven *Risikoausgleich* unter Pkt. 1 (Einleitung).

Bei Werbemaßnahmen auf Basis des berechtigten Interesses ist im Rahmen der Interessenabwägung besonders zu berücksichtigen, dass es sich bei Minderjährigen um eine besonders schutzwürdige Personengruppe handelt.

5.5. Abgrenzung des Anwendungsbereiches der automatisierten Einzelfallentscheidungen

Versicherer setzen bei der Verarbeitung von elektronisch erstellten Versicherungsanträgen und von Schadenmeldungen zum Teil automatisierte Prüfprogramme ein, um eine möglichst rasche Antragsbearbeitung sowie Schadenerledigung zu gewährleisten und auf diese Weise die *Kunden* von den Vorteilen der Digitalisierung (effiziente und effektive Erledigung, deutliche Verkürzung der Bearbeitungszeiten) profitieren zu lassen. Beispielsweise berechnet der Versicherer anhand der im Antrag gemachten Angaben zum Risiko die Höhe der Versicherungsprämie im Regelfall automatisiert und prüft teilweise automatisiert, ob er das beantragte Risiko entsprechend den Annahmerichtlinien übernehmen kann.
Wenn eine vollautomatisierte Verarbeitung keine Beeinträchtigung der Rechtsposition des Betroffenen zur Folge hat, so ist mangels Beschwer das Eingreifen einer natürlichen Person iS des Art. 22 Abs. 3 DSGVO obsolet. Beispiele hierfür im Versicherungsbereich sind insbesondere die automatisierte Polizzierung eines Versicherungsantrags ohne Abweichungen vom Antrag und die automatisierte Erledigung eines Schadensfalls in der Form, dass der Betroffene die Leistung entsprechend dem vertraglich vereinbarten Deckungsumfang erhält. Falls Versicherungsanträge und Schadensfälle nicht im obigen Sinne erledigt werden können, wird entweder eine manuelle Prüfung vorgenommen, sodass keine ausschließlich automatisierte Verarbeitung im Sinne des Art. 22 DSGVO vorliegt, oder die vollautomatisierte Einzelfallentscheidung erfolgt unter Berücksichtigung der Bestimmungen des Art. 22 DSGVO. Dazu zählt gemäß Art. 22 Abs. 3 DSGVO insbesondere das Recht auf Erwirken des Eingreifens einer natürlichen Person durch Kontaktaufnahme mit den bei den Versicherungen etablierten Beschwerdestellen[6] bzw. Kundenservicestellen. Unberührt hiervon bleiben die sonstigen zur Abhilfe bereitstehenden Rechtsinstitute (z.B. "Deckungsklage").
Teilautomatisierte Verarbeitungen sind jedenfalls keine Anwendungsfälle des Art. 22 DSGVO, da in diesen Fällen menschliche Entscheidungen über das Begehren stattfinden. Dazu gehört vor allem die manuelle Antrags- bzw. Schadenfallprüfung durch Mitarbeiter des Versicherers.

6. Informationspflichten bei der Datenerhebung (Artikel 13 und 14 DSGVO)

Der Versicherer informiert betroffene Personen über die Erhebung und Verarbeitung ihrer personenbezogenen Daten, sofern die betroffenen Personen nicht bereits über diese Informationen verfügen. Der Umfang und der Zeitpunkt der Information variieren je nachdem, ob die personenbezogenen Daten direkt bei der betroffenen Person erhoben werden (Art. 13 DSGVO) oder aus einer anderen Quelle stammen (Art. 14 DSGVO).

Im Zuge des Versicherungsgeschäftes sind dabei zumindest folgende unterschiedliche Gruppen von betroffenen Personen relevant: *Kunden* und Interessenten, Dritte im Zusammenhang mit einer Versicherung, die nicht selbst Vertragspartner sind (*Bezugsberechtigte*, *versicherte Personen*, Schädiger, *Geschädigte*, Zeugen), Besucher der Internetseite, Teilnehmer an Veranstaltungen, Gewinnspielen usw.

[6] Versicherer unterliegen aufsichtsrechtlichen Vorgaben zur Einrichtung eines Beschwerdemanagements (EIOPA-BoS-12/069 DE Leitlinien zur Beschwerdebearbeitung durch Versicherungsunternehmen)

Der Versicherer erstellt eine *Datenschutzinformation*, die in präziser, transparenter, verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache die von der DSGVO geforderten Informationen enthält. Es ist möglich, diese *Datenschutzinformation* jeweils an die unterschiedlichen Zielgruppen anzupassen (z.B. *Versicherungsnehmer*, Besucher der Internetseite).

Diese *Datenschutzinformation* wird an leicht auffindbarer Stelle auf dem öffentlich zugänglichen Onlineauftritt des Versicherers und/oder in Form eines Informationsblattes zur Verfügung gestellt. Dies kann auch in stufenweiser Granularität erfolgen (z.B. Kurzinformation mit Verweis auf die ausführliche Information auf der Website) um den *Kunden* eine übersichtliche *Datenschutzinformation* zur Verfügung stellen zu können. Der Versicherer stellt sicher, dass ein Hinweis zur Auffindbarkeit (z.B. Internetlink) der *Datenschutzinformation* bei allen relevanten Dokumenten, auf denen personenbezogene Daten erhoben werden (z.B. Versicherungsantrag) an leicht auffindbarer Stelle enthalten ist.

Versicherer erheben gemäß Art. 14 DSGVO auch ohne Mitwirkung der betroffenen Person personenbezogene Daten, wenn dies im Zusammenhang mit der Begründung, Durchführung oder Beendigung von Versicherungsverhältnissen und insbesondere auch zur Prüfung und Bearbeitung von Leistungsansprüchen erforderlich ist. Dies gilt beispielsweise, wenn der *Versicherungsnehmer* bei Gruppenversicherungen zulässigerweise die Daten der *versicherten Personen* oder bei Personenversicherungen die Daten der *Bezugsberechtigten* angibt oder wenn Angaben über den *Geschädigten*, Schädiger oder Zeugen gemacht werden. Erweist sich die Erteilung der Information als unmöglich oder nur mit unverhältnismäßigem Aufwand (da im Regelfall keine ausreichenden Kontaktdaten vorhanden sind), dann erfolgt keine Information (z.B. bei *versicherten*- und mitversicherten *Personen*, *Bezugsberechtigten*, Zeugen und *Geschädigten*). Ungeachtet dessen informieren die Versicherer in öffentlicher Weise, vorzugsweise auf deren Webseiten, über die im Versicherungsbereich bestehende Notwendigkeit sowie über die Anwendungsfälle derartiger Datenerhebungen.

Die Information unterbleibt auch, wenn die personenbezogenen Daten ihrem Wesen nach, insbesondere wegen des überwiegenden berechtigten Interesses eines Dritten, geheim gehalten werden müssen. Hier kommen im Versicherungsbereich neben den allgemeinen unternehmerischen und gesondert vertraglich vereinbarten Geschäftsgeheimnissen versicherungsspezifisch die Geheimhaltungsverpflichtungen nach § 321 VAG zur Anwendung. Es ist das klare Verständnis dieses Branchenstandards, dass Informationen und Auskünfte nicht zu einer Verletzung der unter § 321 VAG gesetzlich normierten Geheimhaltungspflicht führen dürfen und dass bei der unter § 321 VAG anlassfallbezogen vorzunehmenden Interessenabwägung nicht zuletzt aufgrund der unter § 321 VAG drohenden Sanktionen in Zweifelsfällen der Geheimhaltungspflicht der Vorrang einzuräumen ist.

Eine Information wird nicht erteilt, wenn dies gemäß Art. 14 Abs. 5 DSGVO vorgesehen ist, dh in der Praxis vornehmlich in solchen Fällen, in denen die betroffene Person über die Informationen bereits verfügt oder wenn aufgrund gesetzlicher Vorschriften Vertraulichkeit zu wahren ist (z.B. keine Information des Betroffenen über eine Geldwäscheverdachtsmeldung).

Grundsätzlich erteilt der Versicherer die Informationen gemäß Art. 14 DSGVO (also insbesondere auch die Quelle der Daten) innerhalb einer angemessenen Frist nach Erlangung, spätestens innerhalb eines Monats. Falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an die Person, oder falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.

Eine Information an betroffene Personen kann unterbleiben, wenn diese rechtmäßig vertreten werden und der Vertreter die Informationen erhalten hat. Dies betrifft beispielsweise nicht volljährige Personen, die von ihrem gesetzlichen Vertreter vertreten werden oder betroffene Personen, die eine Vollmacht zur gewillkürten Vertretung (z.B. Makler,-Rechtsanwalt) erteilt haben.

Aufgrund der komplexen Geschäftstätigkeit von Versicherungen müssen sich diese zur Erfüllung Ihrer Verpflichtungen einer Vielzahl von Auftragsverarbeitern bedienen. Eine Auflistung der Kategorien der herangezogenen Auftragsverarbeiter gemäß Art. 13 und 14 DSGVO ist potentiellen betroffenen Personen so einfach wie möglich (daher im Regelfall über die Webseiten des Versicherers und/oder in ausgedruckten Datenschutzhinweisen) zugänglich zu machen. Aufgrund der im Regelfall bestehenden Vielzahl der herangezogenen Auftragsverarbeiter ändern sich diese typischer Weise regelmäßig. Sofern dies nicht mit unverhältnismäßigem Aufwand verbunden ist, werden auch konkrete Auftragsverarbeiter genannt. Davon unberührt bleibt die Benennung der Empfänger oder Empfängerkategorien im Rahmen einer Datenauskunft gemäß Art. 15 DSGVO, welche in Entsprechung der diesbezüglich abzuwartenden Judikatur des EuGH vorgenommen wird. Eine Auftragsverarbeitung in *Drittländern* ist selbstverständlich nur unter den Voraussetzungen des Kapitels V der DSVGO möglich.

7. Kommunikation in der Versicherungswirtschaft

7.1. Unternehmensinterner Datenaustausch

Einzelne Bereiche und Abteilungen von Versicherern nehmen im Rahmen des Versicherungsbetriebs unterschiedliche Datenverarbeitungsaufgaben zweckgebunden wahr. Dem Effizienzgedanken folgend werden personenbezogene Daten idR in zentralisierten Verfahren (Telefonie, Posteingangsbearbeitung, …) verarbeitet.
Als datenschutzrechtlich Verantwortliche stellen Versicherer dabei sicher, dass die technischen und organisatorischen Maßnahmen den datenschutzrechtlichen Anforderungen entsprechen (inkl. Berechtigungs- und Zugriffssystem, aufbauend auf dem Need-To-Know-Prinzip auf Basis der vorab definierten Stellenbeschreibungen des jeweiligen Mitarbeiters).
Weiterführende Informationen zu Datensicherheitsmaßnahmen sind im Kapitel 11 sowie im Anhang 1 „Datensicherheitskonzept“ zu finden.

Verantwortliche iSd DSGVO sind juristische Personen, nicht jedoch Abteilungen oder sonstige Stellen innerhalb der Versicherer. Sind hierbei mehrere Bereiche betroffen (z.B. Unfall- und Krankenversicherung), so erfolgt der hierfür erforderliche Datenaustausch zwischen den betroffenen Bereichen unter Berücksichtigung des Need-To-Know-Prinzips. Hierbei ist die höchstgerichtliche Rechtsprechung zu berücksichtigen, die in einem mangelnden Austausch von Informationen zu einem Schadensfall innerhalb einzelner Sparten eines Versicherers ein diesem zuzurechnendes Organisationsverschulden festgestellt hat (vgl. etwa OGH 7Ob 254/07i) und somit eine spartenübergreifende Wissenszurechnung verlangt. Daher wird das Need-To-Know-Prinzip im Rahmen dieses Branchenstandards als ein durch die Rechtsprechung begründeter Auftrag zum versicherungsinternen Informationsabgleich verstanden. Dies gilt freilich stets unter Wahrung der datenschutzrechtlichen Zweck- und Verhältnismäßigkeitsprinzipien.

Im Interesse der Versichertengemeinschaft können Versicherer auch aus betrugspräventiven Gründen zur Beurteilung ihrer Leistungspflicht bzw. zur Prüfung, ob und zu welchen Bedingungen ein Vertrag abgeschlossen werden kann, Angaben des Anspruch- bzw. Antragstellers gegebenenfalls intern abgleichen (Art. 6 Abs. 1 lit. f DSGVO bzw. § 11a Abs. 1 Z 1 und 3 VersVG).

Betreibt ein Versicherer neben der Rechtsschutzversicherung noch andere Versicherungssparten, findet aufgrund gesetzlicher Sonderbestimmungen (§ 99 VAG) nur ein eingeschränkter Informationsaustausch zwischen der Rechtsschutzsparte und den anderen Sparten des Versicherers statt. Ein spartenübergreifender Datenaustausch zum Zweck der unaufgeforderten Angebotslegung zu über das bestehende Versicherungsverhältnis hinausgehenden Versicherungsprodukten erfolgt nicht. Siehe dazu auch Punkt 5.3.1. (Evaluierung der Risikosituation und Beratung).

7.2. Kommunikationskonzept für geschäftsübliche versicherungsspezifische Anfragen

Für geschäftsübliche versicherungsspezifische Anfragen abseits datenschutzrechtlicher Auskunftsbegehren iSd Art. 15 DSGVO wurde das im Anhang 2 beiliegende Kommunikationskonzept erstellt.

8. Rechte der betroffenen Person (Artikel 15 - 21 DSGVO)

Der Versicherer informiert betroffene Personen über die ihnen gemäß Art. 15-21 der DSGVO zustehenden Rechte in seiner *Datenschutzinformation*.

Betroffene Personen haben gemäß Art. 15 DSGVO das Recht auf eine Bestätigung, ob sie betreffende personenbezogene Daten verarbeitet werden und können Auskunft über diese personenbezogenen Daten verlangen.

Der Versicherer hat sicherzustellen, dass nur die betroffene Person die sie betreffende Auskunft erhält. Daher kann er bei begründeten Zweifeln an der Identität des Antragsstellers zusätzliche Informationen anfordern, die zur Bestätigung der Identität erforderlich sind (z.B. Ausweiskopie). Die Geltendmachung von Betroffenenrechten durch Bevollmächtigte (z.B. Makler, Rechtsanwalt) erfordert eine Spezialvollmacht im Sinne des §1008 ABGB.

Die Auskunftserteilung an die betroffene Person kann durch Übermittlung einer Übersicht der über sie gespeicherten personenbezogenen Daten erfolgen. Das Auskunftsrecht gemäß Art. 15 DSGVO umfasst nicht die Beauskunftung von Daten, die nicht vorliegen, sondern erst durch weitere - im Regelprozess nicht vorgesehene – Verarbeitungsprozesse entstehen. Daher sind Saldierungen und Summen von Einzahlungen, der Wertstand eines Vertrags zum letzten Jahres- und Monatsultimo oder sonstige, im Regelprozess des Versicherungsbetriebs nicht vorhandene Datenbestände nicht eigens zu erstellen, nur um datenschutzrechtlich beauskunftet werden zu können.[7] Ein Recht auf Kopie besteht gemäß § 3 VersVG für die dort angeführten Dokumente (Versicherungspolizze auf Papier, deren Ersatzurkunde oder um Abschriften der vom *Versicherungsnehmer* oder in seinem Namen in Bezug auf den *Versicherungsvertrag* abgegebenen Erklärungen).

Im Falle einer Weitergabe von personenbezogenen Daten an externe Empfänger ist der Betroffene im Rahmen einer Datenauskunft zu informieren. Dies erfolgt in Form einer Auflistung der konkreten Empfänger oder - falls dies mit unverhältnismäßigem Aufwand verbunden ist – der Empfängerkategorien (z.B. Rückversicherer, andere Versicherer, Sachverständige, Werkstätten, *Versicherungsvermittler*, IT-Dienstleister).

[7] DSB-D122.259/0008-DSB/2015

Personenbezogene Daten werden vom Versicherer im Regelfall elektronisch verarbeitet. Aufgrund verschiedener Zwecke kommt es regelmäßig dazu, dass ein bestimmtes Datum in mehreren Systemen verarbeitet werden muss. Die Auskunftserteilung muss diesbezüglich keine Systeme auflisten, in denen ein bestimmtes Datum in rechtmäßiger Weise verarbeitet wird, sondern nur das Datum selbst. Beispielsweise wird die Anschrift eines *Kunden* regelmäßig in der Kundendatenbank, aber auch im Exkasso/Inkasso System sowie in Backupsystemen verarbeitet werden.

Durch die Auskunft dürfen nicht die Rechte von Dritten beeinträchtigt werden; es sind die Verpflichtungen des Datengeheimnisses diesen gegenüber einzuhalten, welches im Versicherungsbereich um den Geheimnisschutz des § 321 VAG ergänzt wird (Versicherungsgeheimnis). Ebenso besteht das Recht auf Auskunft in der Regel dann nicht, wenn durch die Erteilung dieser Auskunft ein Geschäfts- oder Betriebsgeheimnis des Versicherers bzw. Dritter gefährdet würde (gem. § 4 Abs. 6 DSG).

Die betroffene Person hat das Recht, neben den Daten und etwaigen Empfängern / Empfängerkategorien auch Auskunft über die Verarbeitungszwecke, die Herkunft und die geplante Speicherdauer der verarbeiteten Daten zu verlangen.

Die Datenverarbeitung von personenbezogenen Daten erfolgt durch den Versicherer grundsätzlich zu den im Kapitel „Datenverarbeitung“ angeführten Zwecken, beispielsweise zur Bearbeitung eines Antrages, zur Beurteilung des zu versichernden Risikos, zur Erfüllung der Beratungspflichten (z.B. IDD), zur Prüfung einer Leistungspflicht und für das Prämieninkasso.

Sie erfolgt auch zur Prüfung und Regulierung von Ansprüchen *Geschädigter*, zur Prüfung und Abwicklung von Regressforderungen, zur Entwicklung von Tarifen, Produkten und Services sowie zur Erstellung von Statistiken, zur Versicherungsmissbrauchsbekämpfung, zur Erfüllung gesetzlicher und aufsichtsrechtlicher Verpflichtungen oder zu Zwecken der Werbung sowie der Markt- und Meinungsforschung.
Die konkreten Verarbeitungszwecke der Daten des Betroffenen werden im Rahmen der Auskunftserteilung präzisiert.

Im Falle einer Verarbeitung von unrichtigen oder unvollständigen personenbezogenen Daten hat die betroffene Person das Recht auf Berichtigung oder Vervollständigung, ebenso bei Zweifeln über die Rechtmäßigkeit bzw. Richtigkeit/Vollständigkeit der Daten das Recht auf eine Einschränkung der Verarbeitung bis zur endgültigen Klärung der Rechtmäßigkeit bzw. Richtigkeit/Vollständigkeit.

Bei Datenverarbeitungen aufgrund einer Einwilligung kann diese von der betroffenen Person jederzeit und ohne Grund widerrufen werden. In diesem Fall stellt der Versicherer die Verarbeitung der aufgrund der Einwilligungserklärung verarbeiteten Daten unverzüglich ein und weist die betroffene Person darauf hin, dass die bis zum Zeitpunkt des Widerrufes getätigten Verarbeitungen auch weiterhin rechtmäßig bleiben.

Jede betroffene Person hat das Recht auf Beschwerdeerhebung bei der österreichischen Datenschutzbehörde, hierüber informiert der Versicherer in der *Datenschutzinformation* und soweit gesetzlich vorgesehen bei formellen Beantwortungen gemäß Art. 15-22 DSGVO.

Versicherer haben Daten, die für den Zweck der Erhebung nicht mehr benötigt werden, unter den Voraussetzungen des Art. 17 DSGVO zu löschen. Zur Sicherstellung dieser Verpflichtung hat jeder Versicherer ein Datenlöschkonzept in seinen Prozessen zu implementieren (siehe Kapitel 10 Aufbewahrung der Daten).

Betroffene Personen haben das Recht, die zu ihrer Person verarbeiteten Daten, sofern diese von der betroffenen Person selbst zur Verfügung gestellt wurden, in einem maschinenlesbaren Format (z.B. XML in Ausführung Österreichischer Maklerdatensatz) zu erhalten oder den Versicherer mit der direkten Übermittlung dieser Daten an einen von der betroffenen Person ausgewählten Dritten zu beauftragen, sofern der Empfänger dies aus technischer Sicht ermöglicht und der Datenübertragung weder ein unvertretbarer Aufwand, noch gesetzliche oder sonstige Verschwiegenheitspflichten oder Vertraulichkeitserwägungen von Seite des Versicherers oder von dritten Personen entgegen stehen.

Betroffene Personen können, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die Verarbeitung ihrer personenbezogenen Daten widersprechen, wenn diese aufgrund berechtigter Interessen des Versicherers verarbeitet werden oder weil die Verarbeitung für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist oder in Ausübung öffentlicher Gewalt erfolgt, die dem Versicherer übertragen wurde. In diesem Fall darf die Verarbeitung nur unter Voraussetzungen des Art. 21 Abs. 1 DSGVO fortgesetzt werden.

9. Umgang mit Verletzungen des Schutzes personenbezogener Daten ("Data Breach")

Im Falle einer Verletzung des Schutzes personenbezogener Daten (Data Breach) durch den Versicherer oder dessen Auftragsverarbeiter, z. B. wenn Daten unrechtmäßig übermittelt wurden oder Dritten unrechtmäßig zur Kenntnis gelangt sind, informiert der Versicherer unverzüglich und möglichst binnen 72 Stunden (Fristbemessung gemäß FristenberechnungsVO[8]), nachdem dem Versicherer die Verletzung bekannt wurde, die Österreichische Datenschutzbehörde. Die Datenschutzverletzung wird bekannt, wenn der Versicherer eine hinreichende Gewissheit darüber hat, dass ein Sicherheitsvorfall aufgetreten ist, der zu einer Beeinträchtigung des Schutzes personenbezogener Daten geführt hat. Durch geeignete technische Schutz- sowie organisatorische Maßnahmen, insbesondere sofortige Maßnahmen zur Untersuchung des Vorfalls, ist sicher zu stellen, dass etwaige Beeinträchtigungen rechtzeitig erkannt und Sicherheitsmaßnahmen ergriffen werden können.

Ausgenommen von der Meldeverpflichtung sind Data Breaches, die voraussichtlich zu keinem Risiko für die Rechte und Freiheiten der betroffenen Personen führen. Dies kann z.B. bei einem Falschversand an vertrauenswürdige Empfänger der Fall sein, wenn die Einzelfallbeurteilung aufgrund der Umstände (z.B. Vertrauenswürdigkeit des Empfängers, geringe Anzahl und geringe Kritikalität der Daten, bestätigte Löschung) kein Risiko für den Betroffenen erwarten lässt. Ein Risiko besteht insbesondere dann, wenn zu befürchten ist, dass der Data Breach zu einem Identitätsdiebstahl, einem finanziellen Verlust oder einer Rufschädigung führt.

Von einem Data Breach betroffene Personen werden unverzüglich und gesondert benachrichtigt, wenn dieser voraussichtlich zu einem hohen Risiko für deren persönlichen Rechte und Freiheiten führt. Soweit eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde – etwa wegen der Vielzahl der betroffenen Fälle – so tritt an ihre Stelle eine Information der Öffentlichkeit (z.B. auf der Homepage des Versicherers).

[8] Verordnung (EWG, Euratom) Nr. 1182/71 des Rates vom 3. Juni 1971 zur Festlegung der Regeln für die Fristen, Daten und Termine

Sofern durch Maßnahmen (z.B. technische Verfahren wie Verschlüsselung, Hashfunktionen, abgesicherte Datenverfügbarkeit durch Sicherungskopien oder organisatorische Lösungen) sichergestellt wurde, dass voraussichtlich ein Risiko für die Rechte und Freiheiten der betroffenen Personen in aller Wahrscheinlichkeit nicht besteht, kann eine Benachrichtigung der Österreichischen Datenschutzbehörde beziehungsweise der betroffenen Personen unterbleiben. Die Benachrichtigung der betroffenen Personen unterbleibt in allen Fällen, in denen als Folge des Data Breaches kein hohes Risiko für die betroffenen Personen zu erwarten ist wie auch, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen, es sei denn, dass die Interessen der betroffenen Personen an der Benachrichtigung, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.

In der Benachrichtigung an die betroffenen Personen beschreibt der Versicherer in klarer einfacher Sprache die Art der Verletzung und stellen zumindest folgende Informationen zur Verfügung:

- ✓ den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
- ✓ eine Beschreibung der wahrscheinlichen Folgen des Data Breaches und
- ✓ eine Beschreibung der vom Versicherer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung des Data Breaches sowie gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Aufgrund der unterschiedlichen Ausgestaltung ihrer Verarbeitungsprozesse treffen die Versicherer für den Fall einer Verletzung des Schutzes personenbezogener Daten individuelle, unternehmensinterne Vorkehrungen, die die Einhaltung der gesetzlichen Vorgaben und eine fristkonforme Risikoeinschätzung und, sofern erforderlich, eine fristkonforme Vorfallsmeldung garantieren. Ungeachtet der Frage, ob es sich um einen an die österreichischen Datenschutzbehörde und/oder die betroffenen Personen meldepflichtigen Data Breach handelt, dokumentiert der Versicherer sämtliche Data Breaches einschließlich aller damit im Zusammenhang stehenden Fakten, Auswirkungen und ergriffenen Abhilfemaßnahmen. Durch diese Dokumentation stellt der Versicherer sicher, dass die österreichische Datenschutzbehörde jederzeit die Einhaltung der Bestimmungen dieses Kapitels überprüfen kann.

10. Aufbewahrung der Daten

Der Versicherer bewahrt personenbezogene Daten ausschließlich unter Berücksichtigung der rechtlichen Rahmenbedingungen (insbesondere DSGVO, datenschutzrechtliche Sonderbestimmungen im Versicherungsbereich [VersVG, VAG]) solange in personenbezogener Form auf, wie dies zur Erreichung der festgelegten Zwecke erforderlich ist. Die Grundsätze dieser Datenaufbewahrung werden in typisierter Betrachtung wie folgt festgelegt:

Status	**Zweck der Datenaufbewahrung**	**Dauer der Datenaufbewahrung**	**Erläuterung**
I. Vor Begründung des Vertragsverhältnisses (Vorvertraglichkeit)	Daten (auch Interessentendaten) zur Beurteilung, ob und zu welchen Bedingungen ein *Versicherungsvertrag* geschlossen werden	3 Jahre ab der letzten maschinellen Datenerfassung oder abschließender Erledigung	a)

	kann und zu mit den Versicherungsleistungen in Zusammenhang stehenden Themen: Aufbewahrung zur Dokumentation der Wahrung der geschuldeten Informations- und Beratungspflichten (vgl §§ 130 bis 133, 135a bis 135c VAG).		
I. Vor Begründung des Vertragsverhältnisses (Vorvertraglichkeit)	Aufbewahrung von Daten zur Prüfung von Versicherungsrisiken im Antragsfall im Rahmen des beim VVO geführten Zentralen Informationssystems der österreichischen Versicherungswirtschaft in der Lebensversicherung	5 Jahre ab Eintrag	b)
II. Aufrechtes Vertragsverhältnis	Daten zum versicherten Risiko, zur Schaden- und Leistungsabwicklung, zur Leistungshistorie, zur kalkulierten Prämienhöhe und zum Deckungsumfang	Dauer des aufrechten Vertragsverhältnisses, danach siehe Punkt III	c)
III. Nach Beendigung des Vertragsverhältnisses	Daten gem. II zur Erfüllung vertraglicher und nachvertraglicher Pflichten: Aufbewahrung der Daten zur Beweisdokumentation (vgl § 12 VersVG)	10 Jahre ab Vertragsbeendigung	d)
III. Nach Beendigung des Vertragsverhältnisses	Daten gem. II zur Beurteilung vertraglicher oder nachvertraglicher Ansprüche: Aufbewahrung der Daten zur judikaturgeschuldeten Beweisdokumentation (vgl insbes OGH 7 Ob 107/15h; 7 Ob 221/17a; 7 Ob 22/10a ua)	30 Jahre ab Vertragsbeendigung (Lebensversicherung: ab vereinbartem Vertragsende)	e)
III. Nach Beendigung des Vertragsverhältnisses	Daten gem. II zur Beurteilung vertraglicher oder nachvertraglicher Ansprüche: Unbegrenzte Nachhaftung vertraglich vereinbart	unbegrenzt	e)

a) Erläuterung:

Bereits vor Abschluss eines *Versicherungsvertrages* müssen Versicherer personenbezogene Daten erheben, speichern und weiterverarbeiten, insbesondere zur Prüfung, ob und zu welchen Bedingungen ein *Versicherungsvertrag* abgeschlossen werden kann. Da bereits aufgrund dieses vorvertraglichen Kontakts Ansprüche des *Kunden* resultieren können, auch wenn in der Folge kein *Versicherungsvertrag* zustande kommt, hat der Versicherer je nach Einzelfall ein berechtigtes Interesse oder sogar eine rechtliche Verpflichtung[9] zur Aufbewahrung dieser Daten. Der Versicherer muss regelmäßig gegenüber der Finanzmarktaufsichtsbehörde oder im Anlassfall im Rahmen von Gerichtsverfahren nachweisen, dass er seinen Informations-, und versicherungsrechtlichen Wohlverhaltenspflichten nachgekommen ist und ehrlich, redlich und professionell im bestmöglichen Interesse der *Kunden* handelt. Dies ist nur unter Vorlage von Beratungsprotokollen und anderen Unterlagen aus der Anbahnung eines *Versicherungsvertrags* möglich. Daher bewahren Versicherer auch die Daten aus nicht zustande gekommenen *Versicherungsverträgen* inklusive gesundheitsbezogener Angaben drei Jahre ab der letzten maschinellen Datenerfassung oder abschließender Erledigung auf.

Solange es sich im Rahmen des Aufbaus einer Kundenbeziehung um einen Kontakt mit einem Interessenten handelt, kann dies zu einer potentiell anspruchsbegründenden Phase der Vertragsanbahnung führen (insbesondere Bedarfsanalyse, Vorschlag, Offerte oder Antrag). Da auch in solchen Fällen die Aufbewahrungsinteressen des VAGs zu tragen kommen, werden auch Interessentendaten drei Jahre aufbewahrt. Dies spiegelt insofern auch die schon bislang gepflogene Interessenlage wider, da etwa auch die SA022[10] eine dreijährige Aufbewahrungsdauer in Fällen der Geschäftsanbahnung des eigenen Leistungsangebots anerkannt hatte. Auf berechtigte Aufforderung/Verlangen des Interessenten werden die Daten nach eingehender Prüfung des Anspruchs zuvor gelöscht.

Für Daten von Interessenten aus dem Firmen-/ Großkundenbereich und damit in Zusammenhang stehende Verarbeitung von Daten natürlicher Personen (z.B. Ansprechpartner) gilt eine Aufbewahrungsfrist von zehn Jahren.

b) Erläuterung:

Zum Schutz der Versichertengemeinschaft vor Versicherungsmissbrauch und zur Wahrung der Prämienäquivalenz wird beim VVO das Zentrale Informationssystem der österreichischen Versicherungswirtschaft in der Lebensversicherung geführt. Die Dauer der Aufbewahrung der darin gepflegten Daten belief sich gemäß des durch die Datenschutzbehörde registrierten Systemstands bislang auf sieben Jahre ab Eintrag. Gemäß einer im Zuge der Erstellung des Branchenstandards vorgenommenen rechtlichen Angleichung dieser Aufbewahrungsdauer an die einschlägige Judikatur wird die Speicherdauer auf fünf Jahre ab Dateneintrag festgelegt. Hierdurch wird Einklang mit der Judikatur des Bundesverwaltungsgerichts geschaffen, welches hinsichtlich Bonitätsdatenbanken unter Verweis auf die Kapitaladäquanzverordnung (VO Nr 646/2012) eine fünfjährige Speicherdauer zum Zweck des Gläubigerschutzes für angemessen erachtet.[11] Aufgrund ihrer Wesensgleichheit zum versicherungsrechtlichen Gedanken der Prämienäquivalenz und, damit verbunden, dem Schutzgedanken der prämienzahlenden *Versicherungsnehmer* hat diese Judikatur damit auch für das Zentrale Informationssystem der österreichischen Versicherungswirtschaft in der Lebensversicherung eine rechtliche Orientierung geschaffen.

[9] z.B. Dokumentation der Informations- und Beratungspflichten in §§ 130 – 133, 135a – 135c VAG

[10] SA022: Kundenbetreuung und Marketing für eigene Zwecke in der seinerzeitigen Fassung BGBl. II Nr. 312/2004 (Standard- und Muster-Verordnung 2004); diese Verordnung normierte eine vom Gesetzgeber für adäquat erachtete Interessensbalance zwischen dem datenverarbeitenden Unternehmen und dem Betroffenen. Die seinerzeitige gesetzgeberische Wertung zur dreijährigen Interessentendatenaufbewahrung scheint auch unter der DSGVO angemessen.

[11] Vgl BVwG W258.2216873 und W258.2218465; zuletzt auch W211.2225136.

c) Erläuterung:
Da der *Versicherungsvertrag* ein Dauerschuldverhältnis ist, benötigen Versicherer im Rahmen dieser dauerhaften Vertragsbeziehung wiederholt Schaden- und Leistungsdaten eines *Versicherungsvertrages* für die Beurteilung neuer Schaden- und Leistungsfälle. Dies ist insbesondere bei der Beurteilung zur Deckung und Leistungspflicht bei Folge- oder Dauerschäden der Fall, bei der die bisherige Leistungshistorie – welche Schäden zu welchem Sachverhalt wurden bereits in welchem Umfang übernommen – eine besondere Rolle spielt.

Zur Entscheidung über vertragliche Anpassungen und Fortsetzungen von *Versicherungsverträgen* besteht die Notwendigkeit, neben Daten zur Leistungshistorie die kalkulierte Prämienhöhe und den Deckungsumfang bzw. das jeweils übernommene Risiko von Vertragsvorversionen nachvollziehen zu können, um eine Entscheidungsgrundlage für etwaige Vertragsanpassungen oder Novationen zu gewährleisten.

Zur Erfüllung der Pflichten aus dem *Versicherungsvertrag* und aus Gründen der Nachvollziehbarkeit der im Dauerschuldverhältnis versicherten Risikosituation können daher die dafür erforderlichen Daten zum zugrundeliegenden *Versicherungsvertrag* (dazugehörige Stamm-, Vertrags- und *Schadendaten*) sowie Daten aus mit dem versicherten Risiko zusammenhängenden Verträgen und aus Vertragsvorversionen jedenfalls während des aufrechten *Versicherungsvertrages* und darüber hinaus gemäß Punkt III aufbewahrt werden.

d) Erläuterung:
In Anwendung des Versicherungsvertragsgesetzes (insbesondere § 12 VersVG) hat der Versicherer *Vertragsdaten* während des Zeitraums, in dem Ansprüche gegen ihn erhoben werden, gemäß der bestehenden, absoluten Verjährungsbegrenzung, das sind zehn Jahre nach Vertragsende, aufzubewahren.

Erledigungen zu Schaden- und Leistungsfällen nach Beendigung des *Versicherungsvertrages* führen zu einer Verlängerung der zu wahrenden Aufbewahrungsfristen um zehn Jahre ab Erledigung, da diesbezüglich die Verjährungsfrist des § 12 VersVG neu zu laufen beginnt.

e) Erläuterung:
In bestimmten Konstellationen (z.B. in der Haftpflichtversicherung, der Rechtsschutzversicherung und bei bereicherungsrechtlichen Ansprüchen) können Ansprüche gegen den Versicherer nach aktueller Rechtsprechung[12] oder bei vertraglich vereinbarter zeitlich unbegrenzter Nachhaftung bzw. Nachdeckung bis zu dreißig Jahre nach Vertragsende oder noch länger geltend gemacht werden. In diesen Fällen muss der Versicherer Daten aus dem zugrundeliegenden *Versicherungsvertrag* daher dreißig Jahre oder unbegrenzt aufbewahren. Andernfalls hätte der Versicherer im Anlassfall keinerlei Unterlagen zur Verteidigung seiner Rechtsansprüche zur Verfügung.

Wegen der einer Lebensversicherung besonders inhärenten Gefahr von Doppel- und Mehrfachzahlungen wird hier auf den Beendigungszeitpunkt der ursprünglich vereinbarten Versicherungslaufzeit abgestellt.

[12] OGH 7 Ob 107/15h („ewiges" Rücktrittsrecht in der Lebensversicherung bei fehlender/falscher Rücktrittsbelehrung), OGH 7 Ob 221/17a (Nebenleistungspflicht nach § 3 VersVG zur Herausgabe von Vertragsunterlagen besteht nach Vertragsende bei unklarer Rechtslage solange, bis diese durch Gesetz bzw. Judikatur geklärt wird), OGH 7 Ob 22/10a (Schadenmeldung in der Rechtschutzversicherung ist auch nach Ablauf einer vertraglichen einjährigen Ausschlussfrist nach Vertragsende rechtzeitig, wenn den VN an der verspäteten Meldung kein Verschulden trifft).

Generelle Erläuterung:

(i) Die in diesem Branchenstandard dargelegten Aufbewahrungsfristen sind typisierende Aufbewahrungsfristen. Das bedeutet, jeder Versicherer legt unter Heranziehung dieser typisierenden Aufbewahrungsfristen eigenständig für seine Verarbeitungszwecke fest, wie lange welche Daten in seinem Unternehmen gespeichert werden. Durch die Festlegung der für seinen Geschäftsbetrieb angemessene Aufbewahrungsfristen und auch durch die Ergreifung geeigneter technischer und organisatorischer Maßnahmen stellt der Versicherer sicher, dass die für den jeweiligen Verarbeitungszweck vorgehaltenen personenbezogenen Daten auf das notwendige Minimum reduziert werden und die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden.

(ii) Den dargelegten Aufbewahrungsfristen ist inhärent, dass die Datenaufbewahrung neben den angeführten Aufbewahrungspflichten oftmals auch der Beweissicherung zur Abwehr oder Verfolgung von Rechtsansprüchen des Versicherers dient. Der Judikatur geschuldet handelt es sich hierbei oftmals um lange Aufbewahrungsfristen. Im Sinne eines datenschutzrechtlichen Interessenausgleichs erfolgt die Datenaufbewahrung zweckgebunden zur Verwirklichung des dargelegten Nachweisinteresses des Versicherers im Anlassfall. Das bedeutet, dass der Versicherer die aufbewahrten Daten nur zu diesen Aufbewahrungszwecken oder zu damit in Zusammenhang stehenden Zwecken aufbewahrt (wie etwa zur Prüfung, ob ein geltend gemachter Anspruch bereits durch andere Leistungen präjudiziert worden ist) und nur anlassfallbezogen (z.B. in Fällen der Anspruchserhebung) verwendet. Hierzu kann als zusätzliche Sicherheitsmaßnahme insbesondere iSd Datenminimierung z.B. eine Einschränkung des Zugriffs (Sperre) oder eine Verwahrung getrennt vom übrigen Datenbestand vorgesehen werden.

(iii) Ein Versicherungsverhältnis kann auf vielfältige Weise beendet werden, so beispielsweise durch Zeitablauf, Rücktritt oder durch Stornierung (Kündigung). Im Sinne dessen gilt jegliche Form der Beendigung eines einmal begründeten Versicherungsverhältnisses als eine Vertragsbeendigung, an welche die hierfür unter Kategorie III definierten Aufbewahrungsfristen knüpfen. Dies unabhängig davon, ob die Beendigung in zivilrechtlicher Sicht ex tunc (z.B. im Rücktrittsfall) oder ex nunc (z.B. im Kündigungsfall) wirkt.

(iv) Im Rahmen der Anbahnung, des Abschlusses und der Abwicklung von *Versicherungsverträgen* ist es oftmals erforderlich auch Daten dritter Personen, die nicht *Versicherungsnehmer* sind, zu erheben und zu verarbeiten. Dies betrifft vor allem *versicherte Personen*, *Bezugsberechtigte*, sonstige Leistungsempfänger, Schädiger, *Geschädigte* und Zeugen. Für die Daten dieser Personen gelten die dargelegten Aufbewahrungsregeln sinngemäß.

(v) Aufgrund des Wesens einer Bündelversicherung bemisst sich die Dauer der Aufbewahrung ab Beendigung des Bündels anhand der längsten Aufbewahrungsfrist der Vertragsteile.

(vi) Unabhängig von den oben genannten Fristen ist die Löschung von personenbezogenen Daten in bestimmten Fällen vorläufig ausgesetzt, z.B. wenn diese in gerichtlichen, außergerichtlichen oder verwaltungsbehördlichen Verfahren relevant sind. In diesem Fall richtet sich die konkrete Speicherdauer nach dem jeweiligen Anlassfall.

(vii) Nach Wegfall der Aufbewahrungsfrist oder des entsprechenden Aufbewahrungszweckes löscht der Versicherer die Daten. Der Löschung gleichgestellt ist eine Anonymisierung, die den Personenbezug unwiderruflich beseitigt, indem die Rekonstruktion des Personenbezugs nicht oder nur mit einem unverhältnismäßigen Aufwand möglich wäre.

11. Datensicherheit

11.1. Grundsätze der Datensicherheit

Der Versicherer verarbeitet die personenbezogenen Daten unter Berücksichtigung der gesetzlichen Rahmenbedingungen sowie entsprechend den schutzwürdigen Interessen der betroffenen Personen und jenen

des Versicherers. Unter Berücksichtigung des Stands der Technik, der diesbezüglichen Implementierungskosten, des Risikos für die Rechte und Freiheiten betroffener Personen, sowie des Schutzbedarfs des Unternehmens, trifft der Versicherer geeignete technische und organisatorische Maßnahmen (inklusive personeller Maßnahmen), um ein dem jeweiligen Risiko, sowie dessen Eintrittswahrscheinlichkeit, angemessenes Schutzniveau zu gewährleisten. Diesbezügliche Details sind im Anhang 1 „Datensicherheitskonzept“ zu finden.

11.2. Sichere E-Mail-Kommunikation

Der Versicherer setzt zur Erfüllung der Datenschutzvorschriften betreffend Datensicherheit im Zuge der E-Mail Kommunikation auf Transportverschlüsselung (TLS-Version entsprechend dem Stand der Technik) Daten, die der Versicherer mit anderen Kommunikationspartnern per E-Mail austauscht, werden somit nach Stand der Technik verpflichtend verschlüsselt übertragen, dies inkludiert sensible Daten (z.B. Gesundheitsdaten). Sofern der E-Mailprovider des Kommunikationspartners ebenfalls TLS unterstützt, erfolgt jegliche Kommunikation per E-Mail, auch mit *Kunden* und anderen Dritten, verschlüsselt.

Sollte eine Transportverschlüsselung technisch nicht möglich sein, nutzt der Versicherer andere sichere Technologien (wie z.B. verschlüsselte Datenplattformen oder Portallösungen) um die erhöhten Anforderungen gerecht zu werden. Sollte in Ausnahmefällen keine elektronische Kommunikation möglich oder nicht erwünscht sein, nutzt der Versicherer den postalischen Kommunikationsweg.

12. Überwachung der Einhaltung der Verhaltensregeln

1. Eine Überwachungsstelle wird in Form einer unabhängigen Organisationseinheit innerhalb des VVO als die zuständige Einrichtung zur Überwachung der Einhaltung der vorliegenden Verhaltensregeln gemäß Art. 41 DSGVO eingerichtet.
2. Jedes diese Verhaltensregeln unterzeichnende Unternehmen verpflichtet sich zur Anerkennung der Empfehlungen und Entscheidungen dieser Überwachungsstelle.
3. Die genauen Kriterien zur Bestellung der Mitglieder der Überwachungsstelle sowie zu deren Tätigkeit werden in einer separaten Geschäftsordnung festgelegt. Diese kann unter www.vvo.at/coc abgerufen werden.

13. Anhänge

13.1. Anhang 1: Datensicherheitskonzept

13.2. Anhang 2: Kommunikationskonzept