Code of Conduct

Verhaltensregeln gem. Artikel 40 EU-Datenschutz-Grundverordnung

für Versicherungsmakler und Berater in Versicherungsangelegenheiten

Stand: August 2021

Fachverband Versicherungsmakler und Berater in Versicherungsangelegenheiten
Stubenring 16 / Top 7
1010 Wien,
Österreich
Telefon +43 5 90 900 4816
Fax +43 5 90 900 118225
E-Mail ihrversicherungsmakler@wko.at
Webhttps://wko.at/ihrversicherungsmakler

Präambel

Der Fachverband Versicherungsmakler und Berater in Versicherungsangelegenheiten der Wirtschaftskammer Österreich (im Folgenden kurz „Fachverband“) ist die gesetzliche Interessenvertretung der Versicherungsmakler und Berater in Versicherungsagenden gem § 94 Z 76 Gewerbeordnung 1994 (GewO), im Folgenden kurz „Versicherungsmakler“ genannt. Gem § 47 Abs 1 iVm § 43 Abs 3 Wirtschaftskammergesetz (WKG) hat der Fachverband im eigenen Wirkungsbereich die fachlichen Interessen der Branche zu vertreten und den betroffenen Unternehmen rechtliche Beratung und Information zukommen zu lassen.

Der Fachverband hat diese Verhaltensregeln gem Art 40 Datenschutz-Grundverordnung (DSGVO) in Zusammenarbeit mit Vertretern der Branche erstellt (im Folgenden „Verhaltensregeln“ bzw kurz „CoC“). Diese Verhaltensregeln spiegeln die Besonderheiten der einzelnen Verarbeitungsbereiche der Branche und die besonderen Bedürfnisse von Ein-Personen-Unternehmen, Kleinstunternehmen sowie kleinen und mittleren Unternehmen wider und präzisieren dahingehend die Anwendung der DSGVO bzw deren Umsetzungsbestimmungen im Datenschutzgesetz (DSG). Unumgänglich ist somit auch die Beschäftigung mit dem Maklergesetz (MaklerG) und dem Versicherungsvertragsgesetz (VersVG), welches spezielle Bestimmungen datenschutzrechtlicher Art für Versicherungsmakler mit sich bringt. In diesem Sinne erwartet sich der Fachverband Versicherungsmakler Rechtsicherheit und sohin konkreten Nutzen in der korrekten Verarbeitungstätigkeit der Versicherungsmakler.

§ 1 Anwendungsbereich

(1) Die vorliegenden Verhaltensregeln sind für sämtliche Datenverarbeitungen personenbezogener Daten durch juristische oder natürliche Personen mit der Gewerbeberechtigung der Versicherungsvermittlung gem § 94 Z 76 GewO und der Zugehörigkeit zum Fachverband Versicherungsmakler anwendbar.

(2) Es muss eine aktive Verpflichtungserklärung nach § 13 (2) CoC von Seiten des Versicherungsmaklers abgegeben worden sein.

(3) Die Verhaltensregeln beschränken sich auf Verarbeitungstätigkeiten im Inland.

§ 2 Begriffsbestimmungen

(1) **Versicherungsmakler**: Versicherungsmakler und Berater in Versicherungsangelegenheiten gem § 94 Z 76 Gewerbeordnung 1994 (GewO) sind Mitgliedsunternehmen des Fachverbands Versicherungsmakler und Berater in Versicherungsangelegenheiten. Sie agieren wirtschaftlich und rechtlich unabhängig vom Versicherer. Der Versicherungsmakler und Berater in Versicherungsangelegenheiten wird sowohl für den Versicherungskunden als auch für den Versicherer tätig, vertritt jedoch überwiegend die Interessen des Versicherungskunden und unterliegt den Bestimmungen des Maklergesetzes, insbesondere den §§ 26 – 32 MaklerG.

(2) **Auftraggeber der Versicherungsmakler**: Auftraggeber sind Privatpersonen, freiberuflich Tätige, Landwirte, gewerbliche und industrielle Unternehmen, Vereine und Körperschaften, kurz „Kunden“ oder „Auftraggeber“ genannt und nicht mit dem vormals datenschutzrechtlichen Auftraggeber gem DSG 2000 zu verwechseln. Im MaklerG werden diese auch „Versicherungskunden“ genannt.

(3) **Versicherer:** Der Versicherer bzw das Versicherungsunternehmen ist Produzent und Anbieter von Versicherungsprodukten gem Art 2 Z 6 Richtlinie 2016/97 des Europäischen Parlaments und des Rates vom 20. Januar 2016 über Versicherungsvertrieb (IDD) iVm Art 13 Z 1 Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II).

(4) **Score-Wert**: Mit Score-Wert ist die Berechnung der Bonität bzw einer allfälligen wahrscheinlichen Zahlungsfähigkeit / eines potentiell möglichen Zahlungsausfalls gemeint.

§ 3 Rollenbild

(1) Versicherungsmakler können grundsätzlich im Rahmen ihrer gewerblichen Tätigkeit als

i. eigenständige Verantwortliche iSd Art 4 Z 7 DSGVO, sofern allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entschieden wird,

ii. als Auftragsverarbeiter iSd Art 4 Z 8 DSGVO, sofern die personenbezogenen Daten im Auftrag eines anderen Verantwortlichen verarbeitet werden, oder

iii. als gemeinsame Verantwortliche iSd Art 26 DSGVO, sofern zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen, auftreten.

(2) In welcher konkreten Rolle der Versicherungsmakler auftritt, bestimmt sich nach den Umständen des Einzelfalls und ist danach zu beurteilen, wer die wesentliche Entscheidung über die Datenverarbeitung, den Zweck, die Mittel und die Reichweite dieser trifft.

(3) Zu beachten gilt, dass es sich hierbei oftmals um eine Dreiecksbeziehung handelt, da dem Versicherungsmakler eine Vermittlungsposition gegenüber Auftraggeber und Versicherungsunternehmen zukommt. Letztere werden im Regelfall als eigenständige Verantwortliche iSd Art 4 Z 7 DSGVO einzuordnen sein. Eine gemeinsame Verantwortung iSd Art 26 DSGVO kommt regelmäßig nicht in Betracht, da individuell und nicht gemeinsam über Zwecke der und Mittel zur Datenverarbeitung personenbezogener Daten des Auftraggebers entschieden wird.

(4) In der Regel sind Versicherungsmakler bei der Ausübung ihrer gewerblichen Tätigkeit als eigenständige Verantwortliche iSd Art 4 Z 7 DSGVO einzuordnen. Dies deshalb, da ihnen eine wesentliche Entscheidungsbefugnis über Zwecke und Mittel der Verarbeitung personenbezogener Daten zukommt, keine Weisungsgebundenheit besteht und Versicherungsmakler üblicherweise Daten aufgrund rechtlicher Bestimmungen unabhängig von den vermittelten zivilrechtlichen Auftragsverhältnissen aufzubewahren haben. In seiner Tätigkeit ist der Versicherungsmakler unabhängig. Der Versicherungsmakler ist in erster Linie ein unabhängiger Einkäufer von Versicherungsschutz im Interesse seines Auftraggebers (Kunden). Er ist gesetzlich verpflichtet, seinem Kunden bestmöglichen Versicherungsschutz zu vermitteln. Dies kann nicht mit Art 4 Z 8 bzw Art 28 DSGVO in Einklang gebracht werden.

§ 4 Verarbeitungstätigkeiten & Rechtmäßigkeit der Verarbeitung schlicht-personenbezogener Daten

(1) Die Hauptaufgaben des Versicherungsmaklers liegen in der optimalen Beratung des Versicherungskunden und der Vermittlung des nach den Umständen des Einzelfalls bestmöglichen Versicherungsschutzes und umfassen je nach Beauftragung insbesondere folgende Tätigkeiten:

- die angemessene Analyse der Risiken des Versicherungskunden,
- die Erstellung eines angemessenen Deckungskonzeptes,
- die Vermittlung des bestmöglichen Versicherungsschutzes,
- die Prüfung von Polizzen und Prämienvorschreibungen und
- die Unterstützung im Versicherungsfall (Schäden und Leistungen),
- die laufende Überprüfung der bestehenden Versicherungsverträge und die Unterbreitung geeigneter Vorschläge für eine Verbesserung des Versicherungsschutzes.

(2) Sofern der Versicherungsmakler im Rahmen seiner Beauftragung durch den Versicherungskunden für diesen tätig wird, ist die Verarbeitung der schlicht personenbezogenen Daten regelmäßig durch den Rechtfertigungsgrund der Vertragserfüllung iSd Art 6 Abs 1 lit b DSGVO gerechtfertigt und somit rechtmäßig im Sinne der DSGVO. Dieser Rechtfertigungsgrund der DSGVO umfasst auch bereits das vorvertragliche Stadium. Zu beachten ist jedoch, dass die Verarbeitung nur im Umfang der Beauftragung durch den Rechtfertigungsgrund „Vertragserfüllung“ gerechtfertigt ist.

(3) Der Abgleich mit personenbezogenen Daten um personalisierte Angebote zu erstellen ist (branchen-)weit verbreitet. Hierbei werden Versicherungsmodelle und Angebote durch die Heranziehung personenbezogener Daten des individuellen Kunden entsprechend individualisiert, dh auf seine konkreten Wünsche und Bedürfnisse, aber auch auf dessen konkrete Lebenssituation angepasst. Angebote wie in diesem Fall zu individualisieren und hierfür personenbezogene Daten heranzuziehen, fällt nicht unter Art 22 DSGVO (Näheres hierzu siehe § 9 CoC), da hierbei keine ausschließlich automatisierte Verarbeitung durchgeführt wird. Die Entscheidung, welches konkrete Angebot vorgelegt wird, trifft nach wie vor der Versicherungsmakler. In Betracht kommen mehrere Rechtmäßigkeitsgrundlagen nach Art 6 DSGVO, wie beispielsweise, aber nicht ausschließlich, die Vertragserfüllung, die vorvertragliche Notwendigkeit oder das berechtigte Interesse.

Werden bei einer derartigen Verarbeitungstätigkeit auch sensible Daten iSd Art 9 Abs 1 DSGVO verarbeitet (zB Gesundheitsdaten), ist eine ausdrückliche Einwilligung der betroffenen Person einzuholen. Ein Score-Wert ist für sich alleinstehend kein sensibles Datum iSd Art 9 Abs 1 DSGVO. Solange keine sensiblen Daten bei der Berechnung des Angebots miteinbezogen werden, kommen mehrere Rechtsgrundlagen für diese Datenverarbeitung in Betracht (wie unter Abs 3 ausgeführt zB Art 6 Abs 1 lit b oder f DSGVO).

(4) Sollte der Versicherungsmakler eine Einwilligung der betroffenen Person iSd Art 7 DSGVO benötigen, so muss diese nachgewiesen werden können und folgende Bedingungen erfüllen

- Sie hat in verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache zu erfolgen.

- Sie ist im Vorfeld der beabsichtigten Datenverarbeitung zu erteilen.

- Die Einwilligung kann schriftlich, elektronisch oder mündlich erfolgen.

- Sie muss widerrufbar sein. Die betroffene Person muss auf das Recht, die Einwilligungserklärung jederzeit widerrufen zu können, hingewiesen werden.

- Die Einwilligung muss freiwillig erfolgen.

- Einwilligungsbewusstsein der betroffenen Person ist gefordert, das heißt der Versicherungskunde muss wissen, wozu er seine Einwilligung erteilt. Er muss die Art und den Umfang der Verarbeitung seiner personenbezogenen Daten kennen und begreifen, dass er in diese Verarbeitung einwilligt.

- Die Zwecke der Verarbeitung müssen so präzise wie möglich erfolgen, um sicherzustellen, dass personenbezogene Daten nur für jene Zwecke verarbeitet werden, mit denen die betroffene Person bei der Erhebung gerechnet hat. Eine Konkretisierung angelehnt an jene zur Maklervollmacht ist zweckmäßig.

Treten nachträglich neue Verarbeitungszwecke hinzu, die mit einer Verarbeitung verfolgt werden, muss dafür eine neue Einwilligung eingeholt werden oder eine anderweitige Rechtmäßigkeitsgrundlage iSd Art 6 DSGVO herangezogen werden können.

§ 5 Verarbeitungstätigkeiten & Rechtmäßigkeit der Verarbeitung sensibler Daten iSd Art 9 DSGVO

(1) Sofern der Versicherungsmakler besondere Kategorien personenbezogener Daten iSd Art 9 Abs 1 DSGVO (zB Gesundheitsdaten) verarbeitet, kann er sich nicht auf den Rechtfertigungsgrund der Vertragserfüllung iSd Art 6 Abs 1 lit b DSGVO berufen. Für deren Verarbeitung benötigt der Versicherungsmakler eine Rechtsgrundlage iSd Art 9 Abs 2 DSGVO.

(2) Ein Versicherungsmakler hat gem § 28 iVm § 3 Abs 1 und Abs 3 MaklerG die Interessen des Versicherungskunden zu wahren. Dies erfasst in Konkretisierung des unter § 4 Abs 1 CoC aufgelisteten Tätigkeitsbereichs folgendes:

- Aufklärung und Beratung des Versicherungskunden über den zu vermittelnden Versicherungsschutz;
- Erstellung einer angemessenen Risikoanalyse und eines angemessenen Deckungskonzeptes sowie Erfüllung der in den Standesregeln zum Schutz des Versicherungskunden vorgesehenen Dokumentationspflicht;
- Beurteilung der Solvenz des Versicherers im Rahmen der zugänglichen fachlichen Informationen, soweit dies bei der Auswahl des Versicherers zur sorgfältigen Wahrung der Interessen des Versicherungskunden im Einzelfall notwendig ist;
- Vermittlung des nach den Umständen des Einzelfalls bestmöglichen Versicherungsschutzes, wobei sich die Interessenwahrung aus sachlich gerechtfertigten Gründen auf bestimmte örtliche Märkte oder bestimmte Versicherungsprodukte beschränken kann, sofern der Versicherungsmakler dies dem Versicherungskunden ausdrücklich bekanntgibt;
- Bekanntgabe der für den Versicherungskunden durchgeführten Rechtshandlungen sowie Aushändigung einer Durchschrift der Vertragserklärung des Versicherungskunden, sofern sie schriftlich erfolgte; Aushändigung des Versicherungsscheins (Polizze) sowie der dem Vertrag zugrundeliegenden Versicherungsbedingungen einschließlich der Bestimmungen über die Festsetzung der Prämie;
- Prüfung des Versicherungsscheins (Polizze);
- Unterstützung des Versicherungskunden bei der Abwicklung des Versicherungsverhältnisses vor und nach Eintritt des Versicherungsfalls, namentlich auch bei Wahrnehmung aller für den Versicherungskunden wesentlichen Fristen;
- laufende Überprüfung der bestehenden Versicherungsverträge sowie gegebenenfalls Unterbreitung geeigneter Vorschläge für eine Verbesserung des Versicherungsschutzes.

Derartige Tätigkeiten erfordern regelmäßig auch die Verarbeitung besonderer Kategorien von Daten iSd Art 9 Abs 1 DSGVO, insb auch von Gesundheitsdaten.

(3) Darüber hinaus enthält § 11c Z 5 VersVG die Bestimmung, wonach der Versicherer Gesundheitsdaten für die in § 11a Abs 1 VersVG genannten Zwecke an gewillkürte Vertreter des Betroffenen weitergeben darf; dies bedeutet, dass

- zur Beurteilung, ob und zu welchen Bedingungen ein Versicherungsvertrag abgeschlossen oder geändert wird oder
- zur Verwaltung bestehender Versicherungsverträge oder
- zur Beurteilung und Erfüllung von Ansprüchen aus einem Versicherungsvertrag

eine Verarbeitung von Gesundheitsdaten erforderlich ist, um den Gesundheitszustand der betroffenen Person zu erheben und auch die Weitergabe an Versicherungsmakler bzw vice versa (gem § 11 a VersVG) in diesem Zusammenhang rechtmäßig ist. Die Weitergabe der Daten ist daher auf das Verhältnis Versicherer und Versicherungsmakler eingeschränkt. Eine Weitergabe der Daten an Auftragsverarbeiter ist nicht ausgeschlossen. Die jeweilige

Weitergabe der Daten ist dem Kunden nach den allgemeinen Kriterien des Artikel 13 und 14 DSGVO offenzulegen.

Sollte im Falle der automationsunterstützten Übermittlung von Daten iSd Art 9 Abs 1 DSGVO der die Daten empfangende Versicherungsmakler noch nicht im Besitz einer aufrechten Vollmacht der betroffenen Person sein, so muss er unverzüglich nach Kenntniserlangung über den Erhalt der Daten iSd Art 9 Abs 1 DSGVO die betroffene Person kontaktieren und eine Vollmacht einholen, sodass der Versicherungsmakler als gewillkürter Vertreter für die betroffene Person tätig werden kann und hierzu auch die notwendige Verarbeitungstätigkeit vornehmen kann.

(4) Das Zusammenspiel der in den Absätzen 2 - 4 der vorliegenden CoC ausgewiesenen Bestimmungen entspricht Art 9 Abs 2 lit g DSGVO, wonach die Verarbeitung dieser besonderen Kategorien von Daten auf der Grundlage des Rechts des Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist.

(5) Angemessene Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person wurden nicht nur in der Abwägung der besagten Bestimmungen vorgenommen, sondern auch von der Branche selbst. In den Standesregeln für Versicherungsmakler (vgl https://www.wko.at/branchen/information-consulting/versicherungsmakler-berater-versicherungsangelegenheiten/standesregeln.html) sind bereits seit dem 1. Jänner 2017 verstärkte Verschwiegenheitspflichten im § 16ff geregelt.

§ 6 Rechtmäßigkeit der Verarbeitung bei Betriebsübergaben (iSd § 38 Unternehmensgesetzbuch)

(1) Im Rahmen der Vollmacht wird üblicherweise von Seiten des (ursprünglich betrauten) Versicherungsmaklers eine zivilrechtliche Zustimmung eingeholt, dass das Vollmachtverhältnis auch weiter übertragen werden darf, sofern eine Unternehmensübertragung des Versicherungsmaklers stattfindet. Zivilrechtlich ist dies grundsätzlich möglich.

(2) In Zuge der Unternehmensübertragung werden üblicherweise auch schlicht personenbezogene Daten iSd Art 4 Z 1 DSGVO weitergegeben, auf welche der neue Versicherungsmakler direkt Zugriff nimmt. In diesem Falle kann das berechtigte Interesse iSd Art 6 Abs 1 lit f DSGVO oder die Erfüllung der vertraglichen Verpflichtung, welche zivilrechtlich auf den neuen Makler übergegangen ist, iSd Art 6 Abs 1 lit b DSGVO, als taugliche Grundlage für die Weitergabe an den neuen Makler sowie die Verarbeitung durch diesen herangezogen werden.

(3) In der unternehmerischen Praxis wird im Rahmen einer Betriebsübergabe keine direkte Verarbeitung der sensiblen Daten des Versicherungskunden stattfinden, sondern wird vorerst ein technischer Datenabgleich mit den Versicherungen durchgeführt und erst in weiterer Folge werden die Daten beim Versicherungsmakler verarbeitet. Nach herrschender Lehrmeinung muss im Datenschutzrecht zumindest ein „zielgerichtetes Zugreifen“ des Maklers vorliegen. Um von einer „Verarbeitung“ iSd Art 4 Z 2 DSGVO sprechen zu können, ist daher ein aktives Verhalten nötig, um damit einen Zweck der Datenverarbeitung zu definieren.[1]

[1] Vgl *Hödl* in *Knyrim*, DatKomm Art 4 DSGVO Rz 29.

Im Rahmen dieser automatischen Leistungsinformationen bzw Schadeninformationen an den Versicherungsmakler wird ab dem Zeitpunkt der Umstellung der Vermittlernummer, sofern diese Funktion beim Versicherer eingerichtet ist, ein Austausch aller Erledigungs- und Schadeninformationen automatisiert vorgenommen. In diesen automatischen Emails sind bis zu einem gewissen Grad bereits sensible Daten iSd Art 9 Abs 1 DSGVO enthalten. Sobald der Versicherungsmakler die E-Mail zur Kenntnis nimmt, liegt ein zielgerichtetes Zugreifen vor.

(4) Hinsichtlich sensibler Daten iSd Art 9 Abs 1 DSGVO geht, sofern eine rechtsgültige versicherungsvertragsrechtliche Vollmacht bereits vorlag und sich die Geschäftstätigkeit durch den Unternehmensübergang nicht ändert, die Rechtmäßigkeitsgrundlage iSd § 5 CoC auf den Rechtsnachfolger über.

Grundsätzlich sollte sich der Versicherungsmakler aus Transparenzgründen darum kümmern, vorsorglich (für die Verarbeitungstätigkeit ab Zugriffsmöglichkeit auf sensible Daten) eine erneuerte Vollmacht für die Verarbeitung der Daten eingeholt und den Auftraggeber über den Unternehmensübergang informiert zu haben.

(5) Für den Datenaustausch mit den Versicherern gilt Folgendes:

§ 11c Z 5 VersVG enthält die Bestimmung, wonach Versicherer Gesundheitsdaten für die in § 11a Abs 1 genannten Zwecke an gewillkürte Vertreter des Betroffenen weitergeben dürfen; dies bedeutet, dass

- zur Beurteilung, ob und zu welchen Bedingungen ein Versicherungsvertrag abgeschlossen oder geändert wird oder
- zur Verwaltung bestehender Versicherungsverträge oder
- zur Beurteilung und Erfüllung von Ansprüchen aus einem Versicherungsvertrag

die Weitergabe an gewillkürten Vertreter, idS den Versicherungsmakler (gem § 11 a VersVG), in diesem Zusammenhang rechtmäßig ist. Da entweder die zivilrechtliche Vollmacht auf den Rechtsnachfolger übergegangen ist oder eine erneuerte Vollmacht vorsorglich eingeholt wurde, ist der Datenaustausch gem § 11c Z 5 VersVG demnach zulässig.

(6) Sofern sich die Geschäftstätigkeit durch die Unternehmensübertragung ändert bzw ausgeweitet wird, muss eine Einwilligung iSd Art 9 Abs 2 lit a DSGVO von der betroffenen Person zur Verarbeitung sensibler Daten iSd Art 9 Abs 1 DSGVO bzw eine entsprechende versicherungsvertragsrechtliche Vollmacht eingeholt werden.

§ 7 Speicherbegrenzung & Löschkonzept

(1) Gemäß dem Grundsatz der „Datenminimierung“ (Art 5 Abs 1 lit c DSGVO) müssen Datenverarbeitungen auf jenes Maß eingeschränkt werden, das für die Erfüllung des jeweiligen Zwecks erforderlich ist. Diese Einschränkung ist sowohl im Umfang („Zweckbindungsgrundsatz“) als auch hinsichtlich der Dauer (Grundsatz der „Speicherbegrenzung“) zu beachten. Allgemein ergibt sich für Unternehmen die Notwendigkeit, personenbezogene Daten zu verarbeiten und zu speichern, etwa aus vertraglichen Vereinbarungen, berechtigten Interessen oder gesetzlichen Aufbewahrungspflichten, wie insbesondere dem Unternehmensgesetzbuch (UGB), der Gewerbeordnung (GewO) oder der Bundesabgabenordnung (BAO).

(2) Insb bei der Tätigkeit der Versicherungsmakler besteht die Notwendigkeit, umfassend und weitreichend die Wünsche und Bedürfnisse des Versicherungskunden zu erfragen um

Beratungsfehler auszuschließen. Zu diesem Zwecke dürfen jene personenbezogenen Daten, welche nötig sind um nachweisen zu können, keine Beratungsfehler begangen zu haben, entsprechend den schadenersatzrechtlichen Verjährungsfristen § 1489 Allgemeinen Bürgerlichen Gesetzbuch (ABGB) bis zu 30 Jahre aufbewahrt werden.

(3) Unzulässig sind pauschale, nicht näher begründete Aufbewahrungsdauern (wie zB „30 Jahre Speicherdauer gem ABGB“). Gewählte Speicherdauern müssen im Einzelfall durch einen konkreten Anspruch und das die Frist auslösende Ereignis dargelegt werden können.

(4) Im konkreten Fall müssen Berufsberechtige die Speicherdauer in Entsprechung des Datenminimierungsgrundsatzes eigenständig und eigenverantwortlich festlegen, etwa durch Erstellung eines Löschkonzepts. Dieses Löschkonzept hat jedenfalls zu erfassen: Kategorisierung von Daten nach Rechtsgrundlage und Frist der Löschung, konkrete Ausweisung der Fristen zur Löschung, Beschreibung der Löschprozesse für automationsunterschützte Datenverarbeitung und manuell geführte Akte.

§ 8 Informationspflichten

(1) Den Versicherungsmakler als Verantwortlichen treffen Informationspflichten gem Art 13 und 14 DSGVO gegenüber den betroffenen Personen (zB auch den Kunden). Übermittlungsempfänger sind konkret auszuweisen bzw wenn dies nicht möglich ist, bestmöglich zu klassifizieren bzw zu definieren.

In spezifischen Fällen können Versicherungsmakler eine Ausnahme von den Informationsverpflichtungen geltend machen:

- **Der Auftraggeber (die betroffene Person) verfügt bereits über die Informationen**:

Wie bereits in § 5 CoC ausgewiesen, findet ein regelmäßiger Datenaustausch zwischen Versicherer und Versicherungsmakler statt, welcher gesetzlich verankert ist. Erhält der Versicherungsmakler als Vertreter des Versicherungskunden Daten vom Versicherer kann von der Informationspflicht gem Art 14 Abs 5 lit a und c DSGVO von Seiten des Versicherungsmaklers abgesehen werden.

Weiters findet Art 14 Abs 5 lit a DSGVO im Falle einer Gruppenversicherung Anwendung, sofern der Versicherungsnehmer (zB Arbeitgeber im Falle der Gruppenversicherung der Arbeitnehmer oder Hausverwaltung im Falle der Gruppenversicherung der Eigentümer) die Versicherten bereits über den Datenaustausch mit dem Versicherungsmakler informiert hat. Die jeweiligen betroffenen Personen verfügen bereits über die Informationen, weshalb eine neuerliche Erteilung nicht stattfinden muss.

- **Die Erteilung der Informationen erweist sich als unmöglich oder würde einen unverhältnismäßigen Aufwand erfordern**:

Ein Anwendungsfall des Art 14 Abs 5 lit b DSGVO liegt regelmäßig dann vor, wenn Daten geschädigter Dritter (zB Unfallgegner bei einem KFZ Unfall) vom Auftraggeber (Versicherungskunden) an den Versicherungsmakler zur Abwicklung des Schadensfalles weitergegeben werden und dieser diese Daten wiederum an den Versicherer weitergibt. Die Daten des geschädigten Dritten werden vom Unfallverursacher zur Abwicklung der Deckungszusage des Versicherers benötigt und im Zuge dessen an Versicherungsmakler und Versicherer weitergegeben. Eine datenschutzrechtliche aktive Unterrichtung des geschädigten Dritten würde regelmäßig einen unverhältnismäßigen Aufwand darstellen, zumal Kontaktdaten üblicherweise lediglich für den postalischen Weg offengelegt werden.

(2) Eine besondere Problematik für Versicherungsmakler stellt der Sofortabschluss per Telefon dar.

In diesem Fall sollte die Informationserteilung zweistufig erfolgen. In der ersten Stufe sind mündlich die wesentlichen Informationen zu erteilen:

- Einzelheiten zu den Verarbeitungszwecken,
- Identität des Verantwortlichen,
- Betroffenenrechte,
- Informationen über die wichtigsten Auswirkungen von Verarbeitungen, mit denen die betroffene Person nicht rechnet.

Im Zuge des Gesprächs sollte darauf verwiesen werden, wie bzw wann weitere Informationen erteilt werden. Hier ist die Gestaltung einer Informationserklärung als Datenschutzerklärung auf einer allgemein zugänglichen Website des Versicherungsmaklers praktikabel. Ebenso kann die vollständige Informationserklärung mit Übergabe/ Zusendung der Unterlagen nachgeholt werden.

§ 9 Automatisierte Entscheidung im Einzelfall inkl Profiling iSd Art 22 DSGVO

(1) Der Abgleich mit personenbezogenen Daten um personalisierte Angebote zu erstellen ist branchenweit verbreitet. Angebote zu individualisieren und hierfür personenbezogene Daten heranzuziehen, entspricht zwar grundsätzlich der Begriffsdefinition des „Profiling“ gem Art 4 Z 4 DSGVO, ist jedoch nicht unter Art 22 DSGVO, der automatisierten Entscheidungsfindung im Einzelfall inkl Profiling, zu subsumieren. Diese Verarbeitung stellt regelmäßig keinen gestalterischen Akt mit einer in gewissen Weise abschließenden Wirkung (wie zB der Abschluss eines Vertrages) dar; weiters wird keine Entscheidung im Sinne des Art 22 DSGVO automatisiert getroffen, welche für die betroffene Person rechtliche Wirkung entfaltet bzw diese auf sonstige Art und Weise erheblich beeinträchtigt. Vielmehr ist der Versicherungsmakler selbst im Rahmen der Prüfung derart automatisiert generierter Vorschläge verpflichtet, die Angebote individuell zu prüfen und ggf zu verwerfen.

§ 10 Datensicherheitsmaßnahmen und TOM iSd Art 32 DSGVO

(1) Versicherungsmakler sollten zumindest über jene Datensicherheitsmaßnahmen und technische und organisatorische Maßnahmen gem Art 32 berücksichtigen:

- Information und Schulung allf Mitarbeiter,
- Aufgabenverteilung zwischen allf Mitarbeitern,
- Zutrittsberechtigungen (Betrieb, Büro, Aktenschrank, Serverraum),
- Zugriffsberechtigungen (Firewall, Virenschutz, Passwörter, Fernzugrifftools),
- Protokollierung der Datenverwendung/ Zugriffe,
- Verschlüsselung / Pseudonymisierung soweit möglich,
- regelmäßig erfolgte Datensicherungen,
- regelmäßig erfolgte Überprüfungen der Datensicherungen.

§ 11 Datenschutz-Folgenabschätzung

(1) Eine Datenschutz-Folgenabschätzung ist nur dann erforderlich, wenn eine Form der Verarbeitung „wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt“ (Art 35 Abs 1 DSGVO). Ein solch wahrscheinlich hohes Risiko wird insb dann angenommen, wenn eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gem Art 9 Abs 1 DSGVO vorgenommen wird.

In DSFA-A01 Kundenverwaltung, Rechnungswesen, Logistik, Buchführung bzw DSFA-A04 Kundenbetreuung und Marketing für eigene Zwecke der Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV) werden Verarbeitungstätigkeiten erläutert, für welche keine Datenschutz-Folgenabschätzung notwendig ist, da kein nach Art 35 DSGVO gefordertes hohes Risiko in der Verarbeitungstätigkeit gesehen wird.

Verarbeitung personenbezogener Daten im Rahmen der Geschäftsbeziehung eines Versicherungsmaklers mit Kunden und die damit einhergehenden notwendigen Aufzeichnungen aller die Einnahmen und Ausgaben betreffenden Geschäftsvorgänge erfordern keine Datenschutz-Folgenabschätzung. Ebenso wenig ist diese bei Verarbeitungstätigkeiten von Versicherungsmaklern notwendig, wenn eigenen oder zugekauften Kunden- und Interessentendaten für die Geschäftsanbahnung betreffend das eigene Leistungsangebot sowie zur Durchführung von Werbemaßnahmen und Newsletterversand herangezogen werden.

(2) Das Vorliegen der Wahrscheinlichkeit eines hohen Risikos ist durch Versicherungsmakler insb hinsichtlich einer etwaigen umfangreichen Verarbeitung sensibler Daten iSd Art 9 Abs 1 DSGVO zu prüfen.

Der Schwerpunkt der Tätigkeit eines Versicherungsmaklers liegt, wie oben unter § 4 (1) CoC ausgeführt, in der Regel nicht in der Verarbeitung sensibler Daten iSd Art 9 Abs 1 DSGVO, da diese lediglich begleitend erfolgt und keinen wesentlichen Teil der Tätigkeit einnimmt. Sollte hiervon abweichend ein Schwerpunkt in Verarbeitungstätigkeit des Versicherungsmaklers vorliegen, ist das Kriterium der „umfangreichen Verarbeitung sensibler Daten iSd Art 9 Abs 1 DSGVO“ zu prüfen.

(3) Beispiele einer umfangreichen Verarbeitung kann die Verarbeitung von Kundendaten im gewöhnlichen Geschäftsbetrieb eines Versicherungsunternehmens darstellen. Das Unternehmen eines Versicherungsmaklers ist (vgl auch § 4 und 5 CoC) hingegen keineswegs auf diese Größenordnung ausgerichtet, vielmehr arbeitet der Makler für den jeweiligen Versicherungsnehmer bzw unterstützt Versicherungsunternehmen in einem Teilbereich deren Aufgabengebiete. Selbst der direkte Kontakt mit dem Versicherungskunden erfolgt vielfach nicht einmal automatisiert. Der gewöhnliche Geschäftsbetrieb eines Versicherungsmaklers führt daher zu keiner „umfangreichen Verarbeitung sensibler Daten“.

(4) Weiters wird in DSFA-A12 der Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV) ausgeführt, dass – entsprechend Erwägungsgrund (ErwGr) 91 der DSGVO - selbst eine Verarbeitung von Patientendaten dann nicht als umfangreich gilt, wenn sie durch einen einzelnen Arzt oder sonstigen Angehörigen eines Gesundheitsberufes erfolgt. In diesen Fällen wird daher klargestellt, dass eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben ist. Eine umfangreiche und daher einer Datenschutz-Folgenabschätzung unterliegende Tätigkeit liegt vielmehr bei der Patientenverwaltung bzw Honorarabrechnung von Krankenhäusern, Ärztezentren, Gemeinschaftspraxen, Gesundheitsinstituten, Kuranstalten etc vor.[2] Die Verarbeitungstätigkeit von Unternehmen der Versicherungsmakler sind tatsächlich nicht direkt mit der Verarbeitungstätigkeit einer Arztpraxis vergleichbar, da in letzterem Fall bereits im gewöhnlichen Betrieb eine Vielzahl an sensiblen Daten anfällt und verarbeitet wird. Da diese Verarbeitungstätigkeit nicht als umfangreich eingeordnet wird, so kann

[2] Vgl Erläuterungen zur Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV), Zu DSFA-A12 S 4.

jene eines Versicherungsmaklers, welcher zwar sensible Daten verarbeitet, jedoch schon bereits aus dessen Tätigkeitsumfang und gewerberechtlicher Vorgaben in einem weitaus geringeren Umfang als ein einzelner Arzt dies täte, ebenso wenig als umfangreich eingeordnet werden. Im Umkehrschluss kann sohin die Datenverarbeitung von einzelnen Versicherungsmaklern keine umfangreiche Verarbeitungstätigkeit besonderer Kategorien von Daten iSd Art 9 Abs 1 iVm Art 35 Abs 1 iVm Abs 3 lit b DSGVO darstellen und ist im üblichen Tagesgeschäft keine Datenschutz-Folgenabschätzung durchzuführen.

(5) Sofern tatsächlich eine „umfangreiche Verarbeitungstätigkeit“ iSd Art 35 Abs 3 lit b DSGVO vorliegt ist eine Datenschutz-Folgenabschätzung durchzuführen. Was unter „umfangreicher Verarbeitungstätigkeit“ zu verstehen ist, wird in der DSGVO selbst nicht hinreichend genau definiert. Es wird daher empfohlen, bei mindestens 20 Vollzeit-Mitarbeitern, welche überwiegend besondere Kategorien von Daten iSd Art 9 Abs 1 DSGVO verarbeiten, je selbstständiger Organisation, von einer umfangreichen Verarbeitungstätigkeit auszugehen und eine Datenschutz-Folgenabschätzung durchzuführen.

(6) Sollten zudem beispielsweise neue Technologien oder automatisierte Entscheidungsfindungen iSd Art 22 DSGVO eingesetzt werden, ist eine Datenschutz-Folgenabschätzung durchzuführen.

§ 12 Datenschutzbeauftragter

(1) Ein Datenschutzbeauftragter iSd Art 37 DSGVO ist zu bestellen, wenn die Kerntätigkeit in der umfangreichen Verarbeitung sensibler Daten iSd Art 9 Abs 1 DSGVO besteht. Hierbei wird zusätzlich zum Kriterium der „umfangreichen Verarbeitung“ (vgl auch § 11 CoC) auch das Kriterium einer Kerntätigkeit gefordert.

Die Kerntätigkeit eines Versicherungsmaklers liegt, wie oben unter § 4 (1) CoC ausgeführt, in der Regel nicht in der umfangreichen Verarbeitung sensibler Daten iSd Art 9 Abs 1 DSGVO, da diese lediglich begleitend erfolgt und keinen wesentlichen Teil der Tätigkeit einnimmt. Aus diesem Grund ist davon auszugehen, dass ein Versicherungsmakler grundsätzlich nicht dazu verpflichtet ist einen Datenschutzbeauftragten zu bestellen.

(2) Sollte der Schwerpunkt der Tätigkeit des Versicherungsmaklers jedoch in den Bereichen der Kranken- Unfall-, Ärztehaftpflicht oder Lebensversicherung und daher auch in der Verarbeitung diesbezüglicher unumgänglicher besonderer Kategorien von Daten iSd Art 9 Abs 1 DSGVO liegen, so kann eine Kerntätigkeit vorliegen. In diesen Fällen ist zu prüfen, ob eine umfangreiche Verarbeitung erfolgt.

(3) Was unter „umfangreicher Verarbeitungstätigkeit“ iSd Art 37 Abs 1 lit c DSGVO zu verstehen ist, wird in der DSGVO selbst nicht hinreichend genau definiert. Es wird daher empfohlen, in Fällen des § 12 Abs 2 CoC und bei mindestens 20 Vollzeit-Mitarbeitern, welche überwiegend besondere Kategorien von Daten iSd Art 9 Abs 1 DSGVO verarbeiten, je selbstständiger Organisation, einen Datenschutzbeauftragten zu benennen.

(4) Eine freiwillige Bestellung eines Datenschutzbeauftragten durch einen Versicherungsmakler ist jederzeit möglich.

§ 13 Teilnahmeerklärung und Austritt

(1) Versicherungsmakler, die in den räumlichen und sachlichen Geltungsbereich der Verhaltensregeln fallen und nicht von deren Anwendbarkeit ausgeschlossen sind, haben

die Möglichkeit, sich den Verhaltensregeln und den damit verbundenen Rechtsfolgen durch Erklärung gem Abs 2 zu unterwerfen.

(2) Durch Erklärung verpflichten sich Versicherungsmakler, die Verhaltensregeln in ihrer aktuellen Form bei der Verarbeitung personenbezogener Daten im Rahmen ihrer gewerblichen Tätigkeit einzuhalten. Die Erklärung hat zumindest zu umfassen

- die ausdrückliche Aussage, sich zur Anwendung der Verhaltensregeln zu verpflichten,
- den Namen oder die Firma des Berufsberechtigten, den Sitz oder die Geschäftsanschrift,
- die firmenmäßige Zeichnung,
- die Kontaktdaten (E-Mail, Anschrift, Telefonnummer) des Berufsberechtigten.

(3) Eine Erklärung gem Abs 2 ist an den Fachverband Versicherungsmakler per E-Mail an die Adresse ihrversicherungsmakler@wko.at zu übermitteln. Bei Vorliegen der Voraussetzungen gem Abs 1 wird dem Versicherungsmakler eine Bestätigung über die Anwendbarkeit der Verhaltensregeln per E-Mail an die bekanntgegebenen Kontaktdaten übermittelt. Ab Zugang dieser Bestätigung sind die Verhaltensregeln für den Versicherungsmakler verpflichtend.

(4) Der Fachverband führt ein konstitutives öffentliches Verzeichnis der Versicherungsmakler, die sich den Verhaltensregeln durch Erklärung gem Abs 2 unterworfen haben. Die Verhaltensregeln sind nur auf jene Versicherungsmakler anwendbar, die in diesem Verzeichnis genannt sind.

(5) Über Änderungen der Verhaltensregeln werden Versicherungsmakler, die in dem konstitutiven Verzeichnis gem Abs 4 geführt werden, über die von ihnen bekanntgegebenen Kommunikationswege zwei Wochen vor In-Geltung-Treten der Änderungen informiert.

(6) Ein Austritt aus den Verhaltensregeln erfolgt entweder durch

- Erlöschen der Gewerbeberechtigung,
- Austrittserklärung gem § 13 Abs 8 CoC,
- Ausschluss gem § 15 Abs 6 CoC,
- ein Ruhen der Gewerbeberechtigung ab einer Dauer von zwölf Monaten,
- bei Nichtbezahlung der vorgeschriebenen Kosten trotz erfolgter Mahnung oder
- aufgrund einer Entscheidung der Überwachungsstelle.

(7) Die Verhaltensregeln sind ab dem Austritt eines Versicherungsmaklers für diesen nicht mehr anwendbar. Dies hat keine Auswirkung auf die Anwendbarkeit der Verhaltensregeln auf Handlungen, die vor dem Austritt gesetzt wurden.

(8) Durch Übermittlung einer Austrittserklärung an den Fachverband Versicherungsmakler per E-Mail an die Adresse ihrversicherungsmakler@wko.at können Versicherungsmakler aus den Verhaltensregeln austreten.

Die Erklärung hat zumindest zu umfassen

- die ausdrückliche Aussage, aus den Verhaltensregeln austreten zu wollen,
- den Namen oder die Firma des Versicherungsmaklers,
- den Sitz oder die Geschäftsanschrift,
- die firmenmäßige Zeichnung.

(9) Der Fachverband Versicherungsmakler hat einen Vermerk über den Austritt eines Berufsberechtigten in das konstitutive Verzeichnis aufzunehmen.

§ 14 Überwachungsstelle iSd Art 41 DSGVO

(1) Zur Überwachung der Einhaltung der Verhaltensregeln wird eine unabhängige, von der Datenschutzbehörde akkreditierte Überwachungsstelle gemäß Art 41 DSGVO und der Überwachungsstellenakkreditierungs-Verordnung eingerichtet. Diese Funktion wird für die gegenständlichen Verhaltensregeln unter anderem von der Austrian Standards Plus GmbH ausgeübt.

(2) Bei Wegfall einer gemäß Abs 1 eingerichteten Überwachungsstelle hat der Fachverband für eine zeitnahe Bestellung einer neuen Überwachungsstelle zu sorgen.

(3) Ab Abwendbarkeit der Verhaltensregeln ist die Überwachungsstelle berechtigt, geeignete Maßnahmen zu setzen, um die Einhaltung der Verhaltensregeln zu überwachen und die Anwendung der Verhaltensregeln durch die Versicherungsmakler regelmäßig zu überprüfen. Dies beinhaltet für Versicherungsmakler die Verpflichtung

- Anordnungen der Überwachungsstelle nachzukommen,
- der Überwachungsstelle auf Anfrage Informationen bereitzustellen oder geeignete Dokumente und Urkunden vorzulegen, die die Einhaltung der Verhaltensregeln nachweisen,
- Anfragen der Überwachungsstelle zu beantworten,
- an einem Streitbeilegungsverfahren teilzunehmen, welches die Überwachungsstelle gegebenenfalls aufgrund einer bei ihr eingelangten Beschwerden gem … einleitet.

(4) Geht die Überwachungsstelle davon aus, dass ein Versicherungsmakler gegen die Bestimmungen der Verhaltensregeln verstößt oder wird gegen ihn eine Beschwerde gem … eingebracht, hat die Überwachungsstelle den Versicherungsmakler über den Sachverhalt zu informieren und zur schriftlichen Stellungnahme aufzufordern. Sofern es zur Klärung des Sachverhalts erforderlich ist, kann die Überwachungsstelle durch sonstige Beweisaufnahmen weitere Informationen beim Beschwerdeführer oder Beschwerdegegner einholen.

(5) Die Überwachungsstelle ist berechtigt, Verstöße, Stellungnahmen oder sonstige Beweisaufnahmen der Datenschutzbehörde zur Kenntnis zu bringen.

§ 15 Beschwerdeverfahren

(1) Natürliche Personen können Beschwerden über Verstöße gegen die Verhaltensregeln oder über die Art und Weise, auf die die Verhaltensregeln von Versicherungsmakler angewendet werden, bei der Überwachungsstelle einbringen.

(2) Von einer Beschwerde gem Abs 1 unberührt bleibt das Recht auf Anrufung von Gerichten und das Recht der Beschwerdeführung bei der Datenschutzbehörde.

(3) Beschwerden gem Abs 1 sind bei der Überwachungsstelle einzubringen per E-Mail an: ihrversicherungsmakler@wko.at oder per Post an: Fachverband Versicherungsmakler und Berater in Versicherungsangelegenheiten, Stubenring 16 / Top 7 1010 Wien, Österreich.

Die Beschwerde hat mindestens zu umfassen

- einen Nachweis der Identität der beschwerdeführenden natürlichen Person,

- die Bezeichnung des Versicherungsmaklers, gegen welchen Beschwerde erhoben wird,
- der vorgeworfene Vorstoß des Versicherungsmaklers gegen die Verhaltensregeln,
- Kontaktinformationen der beschwerdeführenden natürlichen Person.

(4) Nach Einlangen der Beschwerde haben der Beschwerdeführer und der Versicherungsmakler drei Monate Zeit, um eine Einigung zu erzielen und die Überwachungsstelle über diese zu informieren. Kommt es in diesem Zeitraum zu keiner Einigung, hat die Überwachungsstelle innerhalb eines weiteren Monats Zeit, über die Beschwerde zu entscheiden.

(5) Stellt die Überwachungsstelle in ihrer Entscheidung eine Verletzung der Verhaltensregeln durch einen Versicherungsmakler fest, hat sie Maßnahmen zu setzen, die geeignet sind, einen Verstoß gegen die Verhaltensregeln verlässlich und endgültig abzustellen und eine Wiederholung zu vermeiden. Zur Umsetzung dieser Maßnahmen ist dem Versicherungsmakler eine angemessene Frist zu setzen. Als Maßnahmen können vorgesehen werden

- die Erteilung von Auflagen, verbunden mit der Androhung des Ausschlusses von den Verhaltensregeln, wenn die Einhaltung der Auflagen nicht nachgewiesen wird,
- Anleitungen bzw. Anweisungen, die ein regelkonformes Verhalten ermöglichen,
- die Feststellung über die nicht regelkonforme Verhaltensweise, verbunden mit einer Ursachenfeststellung sowie Lösungsvorschläge für deren Beseitigung, sowie
- der vorläufige oder – im Falle der Wiederholung oder bei schwerwiegenden Verstößen – endgültige Ausschluss von den Verhaltensregeln mit Wirkung.

(6) Das Erheben einer Beschwerde ist für den Beschwerdeführer kostenfrei. Sonstige Kosten, die durch die Verfahrensführung entstehen oder mit dieser in Verbindung stehen, tragen der Beschwerdeführer und der Versicherungsmakler selbst.

(7) Eine Beschwerde kann in derselben Sache nicht gleichzeitig bei der Überwachungsstelle und der Datenschutzbehörde anhängig sein. Erlangt die Überwachungsstelle Kenntnis davon, dass bei der Datenschutzbehörde ein Verfahren in derselben Sache geführt wird, ist das Verfahren bei der Überwachungsstelle mit dieser Begründung einzustellen.