Informationen für Mitglieder

WIRTSCHAFTSKAMMER ÖSTERREICH
Die Versicherungsmakler

Fachverband Versicherungsmakler und
Berater in Versicherungsangelegenheiten

Wirtschaftskammer Österreich

Wien, im Oktober 2017

KURZLEITFADEN für Versicherungsmakler zur Datenschutzgrundverordnung der EU („DSGVO“)

Geschätzte Kolleginnen und Kollegen!
Geschätzte Mitglieder!

Die DSGVO, die im Mai 2018 in Kraft tritt, normiert für alle, die personenbezogene Daten verwenden, verarbeiten, speichern, weitergeben, usw. - auch für Versicherungsmakler - umfassende rechtliche Neuerungen. Gerade Versicherungsmakler, die regelmäßig mit personenbezogenen Daten (z.B. im Zuge der Beantragung des Versicherungsschutzes oder im Rahmen der Schadenabwicklung) arbeiten, ist die frühzeitige Auseinandersetzung mit den neuen datenschutzrechtlichen Regelungen unerlässlich.

Der Fachverband der Versicherungsmakler hat daher unter Involvierung von Rechtsanwalt Dr. Roland Weinrauch und in Zusammenarbeit mit ausgewählten Versicherungsmaklerbüros (insb. Mag. Keltner von der Koban Südvers GmbH) einen Leitfaden ausgearbeitet, der die allgemeinen Informationen, die die WKÖ bereits bereithält, um maklerspezifische Informationen ergänzt.

Zur Erfüllung aller Pflichten sollte der Versicherungsmakler folgende **To Do’s** beachten:

- ⇨ **Überblick über die von ihm verarbeiteten Daten verschaffen und prüfen, auf welchem Rechtfertigungsgrund die Verarbeitung beruht (Vertragserfüllung, Einwilligung, etc.)** → Näheres unter Pkte 4.2. und 5.1.

- ⇨ **Verzeichnis von Verarbeitungstätigkeiten erstellen** → Näheres unter Pkt 5.1.

- ⇨ **(Kunden) Verwaltungssystem nach Gesundheitsdaten durchforsten und Einwilligungserklärungen von den betroffenen Versicherungskunden einholen** → Näheres unter Pkte 4.2 und 4.4.

- ⇨ **Einwilligung für die Zusendung von Marketingmaterial und Newslettern einholen** → Näheres unter Pkt 4.4.

- ⇨ **Informationsblatt erstellen und sowohl auf der Website als auch bei der jeweiligen Beauftragung den Vertragsunterlagen beilegen** → Näheres unter Pkt 5.2.

- ⇨ **Dienstleistungsverträge im Sinne der DSGVO mit allen externen Dienstleistern (= Auftragsverarbeitern) abschließen** → Näheres unter Pkt 3.2.

- ⇨ **In den gemeinsamen Verantwortlichkeitsbereichen Vertrag für gemeinsam Verantwortliche mit den Versicherern abschließen** → Näheres unter Pkt 3.1.a

- ⇨ **Standardisiertes Formular zur Erledigung der Auskunftspflicht anfertigen. Identitätscheck (Ausweiskopie) im Fall begründeter Zweifel vor der Beauskunftung/Löschung/Berichtigung durchführen** → Näheres unter Pkt 5.3.

- ⇨ **Eruieren, welche Datensicherheitsmaßnahmen vorhanden sind. Gegebenenfalls Betriebskonzept erstellen und umsetzen** → Näheres unter Pkt 5.5.

- ⇨ **Prüfen, ob Datenübermittlungen in Drittländer vorliegen** → Näheres unter Pkt 7.

1. Allgemeines zur Geltung

1.1. Ab wann gilt die DSGVO?

Ab 25. Mai 2018. Die DSGVO ist ab diesem Zeitpunkt direkt anwendbar, das heißt eine Umsetzung in österreichisches Recht ist nicht erforderlich. Ab dem 25.Mai 2018 muss jeder Versicherungsmakler die Bestimmungen der DSGVO einhalten.

1.2. Gilt die DSGVO für jeden Versicherungsmakler?

Ja. Ein Versicherungsmakler verarbeitet typischerweise personenbezogene Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

2. Regelungsinhalt

2.1. Welche Daten schützt die DSGVO?

Die DSGVO schützt nur die personenbezogenen Daten von natürlichen Personen. Die Daten von juristischen Personen (Firma, Unternehmenskennzahlen, Bilanzdaten, etc..) sind nicht vom Anwendungsbereich der DSGVO erfasst. Spricht man also von personenbezogenen Daten, meint man immer die Daten von natürlichen Personen.

2.2. Was sind personenbezogene Daten?

Personenbezogene Daten sind definitionsgemäß alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person (= **die betroffene Person** gemäß Terminologie des DSGVO) beziehen. Der Begriff der personenbezogenen Daten ist sehr weit zu verstehen und umfasst Identifikationsmerkmale (zB Name, Anschrift, Geburtsdatum), äußere Merkmale (zB Geschlecht, Augenfarbe, Größe, Gewicht), innere Zustände (zB Meinungen, Wünsche, Überzeugungen) und sachliche Informationen (Vermögens- und Eigentumsverhältnisse, Kommunikations- und Vertragsbeziehungen).

Da auch bereits bei Bestimmbarkeit einer natürlichen Person personenbezogene Daten vorliegen, sind auch Kunden-, Polizzen- und Schadennummern von der Definition umfasst. Grundsätzlich ist somit festzuhalten, dass die meisten Daten, die ein Versicherungsmakler im Rahmen seiner Vermittlertätigkeit verarbeitet, personenbezogene Daten sind.

2.3. Gibt es besonders schutzwürdige Daten im Sinne der DSGVO?

Ja, Art. 9 DSGVO normiert all jene Daten, die der europäische Gesetzgeber für besonders schutzwürdig erachtet. Er bezeichnet diese „sensiblen Daten“ als besondere Kategorien von personenbezogenen Daten. Daten, die zu dieser besonderen Kategorie gehören sind jene Daten, aus denen die rassische und ethnische Herkunft, die politischen Meinungen, die religiösen oder weltanschaulichen Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Sofern diese Daten verarbeitet werden, ist besondere Vorsicht geboten (ausführlicher dazu unter Pkt.4.2.f).

2.4. Wann werden Daten iSd DSGVO „verarbeitet“?

Der Verarbeitungsbegriff ist sehr weit gefasst und erfasst jeglichen Umgang mit personenbezogenen Daten. ZB das Erheben, die Speicherung, das Auslesen, die Weitergabe, die Verknüpfung, die Organisation, das Ordnen, die Anpassung und Veränderung, …

Das heißt, dass der Versicherungsmakler im Rahmen seiner Vermittlertätigkeit immer eine Verarbeitung von (personenbezogenen) Daten im Sinne der DSGVO vornimmt.

3. Adressaten der DSGVO

3.1. Wer ist der sogenannte Verantwortliche im Sinne der DSGVO?

Der Verantwortliche ist eine natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Die DSGVO richtet sich somit unabhängig von der Rechtspersönlichkeit an jenen, der die Verarbeitung der personenbezogenen Daten verantwortet, der also über das Was und das Wie der Verarbeitung entscheidet.

Aus diesem Grund ist jeder Versicherungsmakler, unabhängig davon ob er als Einmannunternehmen oder in Form einer Kapital- oder Personengesellschaft personenbezogene Daten verarbeitet, Verantwortlicher im Sinne der DSGVO.

a. Ist auch der Versicherer Verantwortlicher im Sinne der DSGVO?

Ja, auch der Versicherer entscheidet über die Mittel und Zwecke der Verarbeitung von personenbezogenen Daten. All jene Daten, die der Versicherer verarbeitet, stehen unter seiner Verantwortlichkeit. Das hat zur Folge, dass sowohl der Versicherer als auch der Versicherungsmakler Verantwortliche im Sinne der DSGVO sind.

Es ist davon auszugehen, dass jeder für sich allein Verantwortlicher hinsichtlich seiner personenbezogenen Daten ist und daher alleine die rechtliche Verantwortung für seine Datenverarbeitungen (und die Pflichten gemäß DSGVO) trägt. Es gibt aber auch Bereiche, in denen sie gemeinsam Verantwortliche sind - zB in Bereichen, wo sie die Zwecke der Verarbeitung gemeinsam festlegen und/oder gemeinsam Entscheidungsbefugnis haben. Das bedeutet, dass Versicherer und Versicherungsmakler in diesen Bereichen eine geteilte rechtliche Verantwortung für eine Datenverarbeitung tragen. Gemeinsam Verantwortliche haben in einer Vereinbarung festzulegen, wer welche Verpflichtungen gemäß DSGVO erfüllt (insbesondere Betroffenenrechte, Informationspflichten).

Besonders schwierig und komplex einzuordnen sind Fälle, wo auf Plattformen oder Portalen zusammengearbeitet wird, so zB die Portale der Versicherer. Soweit ein Versicherer diese Infrastruktur alleine einrichtet und damit über ein wesentliches Element der einzusetzenden Mittel alleine entscheidet und alleine über Funktionen, Zugriffe usw entscheidet, ist davon auszugehen, dass hinsichtlich dieser gemeinsam genutzter Portale keine gemeinsame Verantwortung iSd DSGVO vorliegt, sondern der Versicherer allein Verantwortlicher iSd DSGVO ist.

To Do's: Tätigkeitsbereiche/Vorgänge/Tätigkeiten analysieren und in Bereichen gemeinsamer/geteilter Verantwortlichkeiten einen Vertrag mit den Versicherern abschließen.

b. Welche Pflichten hat der Verantwortliche?

Der Verantwortliche hat

- die Einhaltung der DSGVO-Pflichten sicherzustellen
- geeignete technische und organisatorische Maßnahmen zu treffen
- den Nachweis zu erbringen, dass die Verarbeitung DSGVO-konform erfolgt.

Der Verantwortliche hat dafür Sorge zu tragen, dass jede Verarbeitung von personenbezogenen Daten den Grundsätzen der DSGVO entspricht und dass sowohl seine Mietarbeiter, als auch externe Dienstleister mit denen der Versicherungsmakler zusammenarbeitet die Vorschriften der DSGVO einhalten (siehe ausführlicher dazu Pkt. 5).

3.2. Sind auch meine externen Dienstleister von der DSGVO umfasst?

Der Verantwortliche kann zur Verarbeitung der personenbezogenen Daten externe Dienstleister (natürliche oder juristische Personen) heranziehen. Die DSGVO bezeichnet diese Personen als Auftragsverarbeiter.

Ein Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Demnach arbeitet man als Versicherungsmakler beispielsweise dann mit einem Auftragsverarbeiter zusammen, wenn man mit Tarifrechnern, Together oder Chegg.net arbeitet bzw die IT-Infrastruktur (Datenverwaltung, IT-Administration, Wartungsarbeiten, usw.) von externen Dienstleistern nutzt.

Sobald eine derartige Zusammenarbeit vorliegt, muss zwischen dem Versicherungsmakler (Verantwortlicher) und dem externen Dienstleister (Auftragsverarbeiter) ein schriftlicher Vertrag abgeschlossen werden. In diesem Vertrag sind neben Gegenstand und Dauer, Art und Zweck der Verarbeitung sowie Art der personenbezogenen Daten und Kategorien der betroffenen Personen, insbesondere auch dem Auftragsverarbeiter die Pflichten aufzuerlegen, die er gemäß DSGVO zu erfüllen bzw einzuhalten hat.

Die DSGVO räumt die Möglichkeit ein, dass die Europäische Kommission oder die Aufsichtsbehörde „Standardvertragsklauseln" festlegen können, die für den abzuschließenden Vertrag herangezogen werden können. Sobald diese veröffentlicht sind, empfiehlt es sich, auf diese zurückzugreifen.

Den Versicherungsmakler als Verantwortlichen trifft eine Auswahlverantwortung: Er darf nur solche Auftragsverarbeiter heranziehen, die ebenfalls die Bestimmungen der Datenschutzgrundverordnung einhalten und nachweisbar Maßnahmen ergreifen, die dem Schutz der personenbezogenen Daten dienen.

To Do's: Der Versicherungsmakler sollte eine Liste von all seinen externen Dienstleistern (= Auftragsverarbeitern) erstellen und mit diesen einen Dienstleistungsvertrag im Sinne der DSGVO abschließen.

4. Grundsätze der DSGVO

4.1. Welche Grundsätze kennt die DSGVO?

Die Verarbeitung von personenbezogenen Daten muss immer unter Einhaltung folgender Grundsätze erfolgen:

- Rechtmäßigkeit: die Verarbeitung ist nur zulässig wenn ein Rechtfertigungsgrund im Sinne der DSGVO erfüllt ist
- Verarbeitung nach Treu und Glauben
- Transparenz: der Versicherungskunde (betroffene Person) muss nachvollziehen können, in welchem Umfang und auf welche Weise seine Daten verarbeitet werden.
- Zweckbindung: die personenbezogenen Daten dürfen nur für jenen Zweck verarbeitet werden zu dem sie erhoben wurden. Das heißt, dass der Versicherungsmakler die Kundendaten immer nur im Umfang seiner Beauftragung oder im Rahmen der Einwilligung des Versicherungskunden verarbeiten darf
- Datenminimierung: die Verarbeitung von personenbezogenen Daten muss auf das notwendige Maß beschränkt werden
- Richtigkeit: die personenbezogenen Daten müssen richtig sein.
- Integrität und Vertraulichkeit: die Verarbeitung muss derart erfolgen, dass eine angemessene Sicherheit der Daten gewährleistet ist.

4.2. Wie verarbeitet der Versicherungsmakler personenbezogene Daten rechtmäßig?

Sofern der Versicherungsmakler im Rahmen seiner Beauftragung durch den Versicherungskunden für diesen tätig wird, ist die Verarbeitung der personenbezogenen Daten – mit Ausnahme der sensiblen personenbezogenen Daten – grundsätzlich durch den Rechtfertigungsgrund der Vertragserfüllung 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“ legitimiert ist und dass sensible personenbezogene Daten nicht erfasst sind. Sofern der Versicherungsmakler sensible personenbezogene Daten (z.B. Gesundheitsdaten) verarbeitet, kann er sich nicht auf den Rechtfertigungsgrund der Vertragserfüllung berufen. Für deren Verarbeitung benötigt der Versicherungsmakler **jedenfalls eine Einwilligung** der betroffenen Person. Die Einwilligung muss sich explizit auf die Verarbeitung von Gesundheitsdaten beziehen.

Zu beachten ist zudem, dass aufgrund des Grundsatzes der Zweckbindung der jeweilige Rechtfertigungsgrund nur für den konkreten Zweck Wirkung entfaltet. Sofern man die Daten auch für einen anderen Zweck – bspw. Kontaktdaten nicht nur zur Vertragserfüllung, sondern auch für Marketingzwecke/Newsletter – verwenden will, müsste diesbezüglich ebenfalls eine Einwilligung des Versicherungskunden eingeholt werden.
Der Versicherungsmakler muss prüfen, ob die von ihm verarbeiteten Daten durch den Rechtfertigungsgrund der Vertragserfüllung gedeckt sind. Dies wäre bspw nicht der Fall, wenn der Versicherungsmakler den Versicherungsnehmer lediglich in betrieblichen Angelegenheiten betreut, in seinem Kundenverwaltungssystem hingegen auch dessen Hobbys abspeichert, ohne von diesem für den Privatbereich beauftragt zu sein.

To Do's: Der Versicherungsmakler muss prüfen in welchem Umfang er beauftragt ist und ob die Beauftragung die Verarbeitung der Daten rechtfertigt.

4.3. Wie muss eine gültige Einwilligung formuliert sein?

Eine rechtsgültige Einwilligung muss 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 auch mündlich (nicht zu empfehlen wegen Beweispflichten) erfolgen.
- Sie **muss widerrufbar** sein. Die betroffene Person muss auf ihr Recht, die Einwilligungserklärung jederzeit **widerrufen** zu können, hingewiesen werden.
- Die Einwilligung muss freiwillig erfolgen (Wahlfreiheit zur Abgabe der Einwilligung, sie darf keine Voraussetzung dafür sein, dass der Vertrag erfüllt wird).
- **Einwilligungsbewusstsein** der betroffenen Person ist gefordert, das heißt der Versicherungskunde muss wissen, wozu er seine Zustimmung gibt. Er muss die Art und den Umfang der Verarbeitung seiner personenbezogenen Daten kennen und begreifen, dass er in diese Verarbeitung einwilligt.
- **Bestimmtheit**: Der Zweck / 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 Einwilligung muss sich nicht unbedingt nur auf einen einzigen Datenverarbeitungszweck beschränken, sie darf sich auf mehrere Verarbeitungszwecke beziehen. Diese müssen allerdings eindeutig beschrieben, festgelegt und legitim sein.

Treten nachträglich **neue Zwecke** hinzu, die mit einer Verarbeitung verfolgt werden, muss dafür eine neue Einwilligung eingeholt werden.

4.4. Soll der Versicherungsmakler immer eine Einwilligung einholen?

Es ist **nicht zu empfehlen**, den Rechtfertigungsgrund der Einwilligung im Sinne einer „Globaleinwilligung" zu verwenden. Ein Einwilligungs-Disclaimer im Rahmen des Versicherungsmaklerauftrages bzw der Vollmacht kann die Bedingungen der Einwilligung im Sinne der DSGVO nie entsprechen. Ein derartiger Disclaimer ist viel zu unpräzise und kann die Zwecke der Verarbeitung nicht (ausreichend) darstellen.
Zudem ist zu beachten, dass sofern die Einwilligung unwirksam ist oder die Einwilligung verweigert oder widerrufen wird, die Verarbeitung der Daten unzulässig wird.

To Do`s: Kundenverwaltungssystem nach Gesundheitsdaten durchforsten und Einwilligungserklärungen von den betroffenen Versicherungskunden einholen. Zusendung von Marketingmaterial und Newslettern bedarf der Zustimmung des Versicherungskunden.

5. Pflichten gemäß DSGVO

Die DSGVO normiert einen umfangreichen Pflichtenkatalog den der Versicherungsmakler als Verantwortlicher zu erfüllen hat. In der Folge werden hier die wichtigsten Pflichten für Versicherungsmakler dargestellt:

- Verzeichnis von Verarbeitungstätigkeiten Art 30 DSGVO
- Informationspflichten
- Erfüllen der Betroffenenrechte
- Data Breach Notification Art 33 DSGVO
- Maßnahmen zur Datensicherheit

5.1. Muss jeder Versicherungsmakler ein VERZEICHNIS von VERARBEITUNGSTÄTIGKEITEN führen?

Die DSGVO sieht keine Meldung mehr an das Datenverarbeitungsregister (DVR) vor und auch die DVR-Nummer gehört der Vergangenheit an. Stattdessen ist ein Verzeichnis über die Verarbeitung von Daten zu führen (Verarbeitungsverzeichnis Art 30 DSGVO).

Da der Versicherungsmakler personenbezogene Daten „nicht nur gelegentlich" verarbeitet, sondern permanent, hat er auch dann ein Verarbeitungsverzeichnis zu führen, wenn er als Einmannunternehmen agiert. Bei der Verarbeitung sensibler Daten (ua Gesundheitsdaten) ist ausnahmslos ein Verarbeitungsverzeichnis zu führen.

a. In welcher Form ist das Verarbeitungsverzeichnis zu führen?

Es ist schriftlich zu führen. Konkretere Vorschriften gibt es in der DSGVO nicht. Solange am Markt keine Datenbanken angeboten werden oder man sich selber keine Datenbank „bastelt", empfiehlt sich die Führung des Verarbeitungsverzeichnisses in Form einer Exel-Datei.

b. Was muss das Verarbeitungsverzeichnis beinhalten?

- Den Namen und die Kontaktdaten des Verantwortlichen (gegebenenfalls auch des Datenschutzbeauftragten)
- Die Zwecke der Verarbeitung (zu empfehlen: Angabe der Rechtsgrundlage, zB Einwilligung)
- Beschreibung der Betroffenenkategorien
- Beschreibung der Datenkategorien
- Empfängerkategorien
- Wenn möglich die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- Wenn möglich eine allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen

c. Wie könnte der Versicherungsmakler bei Erstellung des Verzeichnisses vorgehen?

Der Versicherungsmakler sollte jeweils eine Liste von

- seinen Verarbeitungstätigkeiten (Versicherungsvermittlung, Schadenbearbeitung, Personalverwaltung, Buchhaltung, Marketing, Email-Newsletter etc.),
- den betroffenen Personengruppen (Kunden, Mitarbeiter, Agenturen, Interessenten, Tippgeber, Kooperationspartner, etc.)
- den durch ihn verarbeiteten Datenkategorien (Namen, Adresse, Geburtsdatum, Polizzennummer, Bankdaten, etc.)

erstellen.

Im Anschluss daran sollte er die Listen zusammenführen, das heißt, die durch ihn verarbeiteten Daten den jeweiligen Verarbeitungstätigkeiten und jeder Verarbeitungstätigkeit den zutreffenden Rechtfertigungsgrund (Vertragserfüllung, Einwilligung, etc.) zuordnen. Auch die jeweiligen Lösch-Fristen (wann soll diese Datenkategorie gelöscht werden), sofern dies möglich ist, müssen Bestandteil des Verzeichnisses sein. Das Ergebnis der Zusammenführung kann bspw in einer Excel-Tabelle dargestellt werden. Die dadurch entstandene „Tabelle“ ist das Verzeichnis von Verarbeitungstätigkeiten im Sinne der DSGVO.

d. Welche Auswirkung hat die Verletzung dieser Pflicht?

Das Verarbeitungsverzeichnis ist absolutes „Muss“ für den Versicherungsmakler und sollte unbedingt ab Geltung der DSGVO im Mai 2018 vorhanden sein. Die Nichtführung eines Verarbeitungsverzeichnisses ist an ein Bußgeld (bis zu EUR 10 Mio bzw 2% des Jahresumsatzes) geknüpft.

To Do: Verzeichnis von Verarbeitungstätigkeiten erstellen.

5.2. Welche INFORMATIONSPFLICHTEN normiert die DSGVO?

Den Versicherungsmakler als Verantwortlichen treffen gewisse Informationspflichten gegenüber den betroffenen Personen (z.B. Versicherungskunden). So hat zum Beispiel der Versicherungsmakler seine Versicherungskunden über seinen Namen und seine Kontaktdaten, über die Verarbeitungszwecke, über die Rechtsgrundlage der Verarbeitung und über die Empfänger der Daten/ Empfängerkategorien (z.B. die Versicherungsgesellschaften) zu informieren.

a. Wann und wie sind die Informationen zur Verfügung zu stellen?

Die Informationen sind zum Zeitpunkt der Erhebung der Daten (= wenn der Versicherungsmakler die Daten von der betroffenen Person erhält) in präziser, transparenter, verständlicher und leicht zugänglicher Form schriftlich, gegebenenfalls elektronisch zu erteilen. Die Information über die Verarbeitung der personenbezogenen Daten muss folgendes enthalten:

- Namen und Kontaktdaten des Verantwortlichen (und ggf seiner Vertreter).
- Verarbeitungszwecke und Rechtsgrundlage der Verarbeitung.
- Empfänger der Daten oder Kategorien der Empfänger (Versicherungskunden, Versicherer, Tippgeber, etc.), die Empfänger müssen nicht namentlich genannt werden.
- Ob die Daten in ein Drittland übermittelt werden.
- Dauer der Datenspeicherung bzw wenn unmöglich die Kriterien für die Festlegung der Dauer.

- Betroffenenrechte
- Die Möglichkeit des Widerrufs der Einwilligung.
- Aufklärung über das Beschwerderecht bei einer Datenschutzbehörde.
- Informationen darüber, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte.
- Ggf Information über das Bestehen „automatisierter Entscheidungsfindung“ (Profilingmaßnahmen).

In der Praxis empfiehlt es sich, ein (Standard-) Informationsblatt vorzubereiten, welches die erforderlichen Informationen enthält. Das Informationsblatt sollte der Versicherungsmakler sowohl dauerhaft auf seiner Website gut ersichtlich platzieren – zB eigener Menüpunkt – sowie bei jeder Beauftragung (Abschluss des Versicherungsmaklervertrages, Erteilung der Vollmacht) das Informationsblatt beizulegen (auch elektronisch möglich). Vergleichbar ist das Informationblatt mit den AGB des Versicherungsmaklers.

Eine besondere Problematik für Versicherungsmakler stellt in diesem Zusammenhang der Sofortabschluss per Telefon dar. Denn eine Erteilung der Informationen nach der Erhebung der Daten, also nach Vertragsabschluss, ist in der DSGVO nicht vorgesehen. Zwar ermöglicht die DSGVO auch die mündliche Informationserteilung, aber nur, wenn dies die betroffene Person (der Versicherungskunde) verlangt.

To Do’s: Informationsblatt erstellen und wie AGB‘s sowohl auf der Website als auch bei der jeweiligen Beauftragung den Vertragsunterlagen beilegen.

b. Muss der Versicherungsmakler diese Informationspflichten auch einhalten, wenn er die Daten nicht direkt bei der betroffenen Person erhebt?

Ja, der Versicherungsmakler muss die Informationspflichten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, spätestens jedoch innerhalb eines Monats erfüllen. Die Daten müssen nicht zur Verfügung gestellt werden, wenn die betroffene Person bereits über die Informationen verfügt.

Das heißt, sobald der Versicherungsmakler personenbezogene Daten eines Versicherungskunden nicht direkt bei diesem, sondern z.B. beim Versicherer anfragt, dann muss er nachträglich den Versicherungskunden informieren, dass er seine personenbezogenen Daten beim Versicherer erhoben hat und muss die Informationen (siehe oben 5.2.) erteilen, es sei denn eine derartige Information ist bereits erfolgt. Die Information wird immer dann bereits erfolgt sein, wenn der Versicherungsmakler mit dem Versicherungskunden in einer aufrechten Geschäftsbeziehung steht und bei Beginn dieser Geschäftsbeziehung seine Informationspflichten gemäß DSGVO erfüllt hat (sowie freilich keine personenbezogenen Daten für einen „neuen“ Zweck erhoben werden; diesfalls wäre der Versicherungskunde darüber zu informieren).

c. Welche Auswirkung hat die Verletzung dieser Pflicht?

Die Verletzung der Informationspflicht ist mit bis zu EUR 20 Mio oder 4% des letztjährigen weltweiten Jahresumsatzes sanktioniert.

5.3. Welche BETROFFENENRECHTE gibt es?

- Recht auf Auskunft (Art 15 DSGVO)
- Recht auf Berichtigung (Art 16 DSGVO)
- Recht auf Löschung ("Recht auf Vergessenwerden") (Art 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art 18 DSGVO)
- Recht auf Datenübertragbarkeit (Art 20 DSGVO)
- Widerspruchsrecht (Art 21 DSGVO)

Von den genannten Rechten wird der Versicherungsmakler im Wesentlichen mit den Rechten auf Auskunft, Berichtigung und Löschung konfrontiert sein.

a. Muss der Versicherungsmakler die Betroffenenrechte immer erfüllen?

Ja, sobald eine betroffene Person ein Betroffenenrecht gegenüber dem Versicherungsmakler geltend macht, muss der Versicherungsmakler die jeweilige Forderung erfüllen, auch wenn diese mehrmals im Jahr gestellt wird. Lediglich wenn dem Auskunftsrecht gesetzliche Beschränkungen entgegenstehen oder das Auskunftsverlangen offenkundig unbegründet oder wegen der Häufigkeit exzessiv ist, darf man die Auskunft verweigern. Allerdings: Der Betroffene ist dennoch innerhalb der Frist zu verständigen und man hat zu begründen, warum man dem Auskunftsverlangen nicht nachkommt. Grundsätzlich gibt es für die Auskunftserteilung keinen Kostenersatz. Nur bei offenkundig unbegründeten oder exzessiven Anträgen eines Betroffenen oder wenn mehrere Kopien übermittelt werden, kann der Versicherungsmakler ein angemessenes Entgelt verlangen.

Hat der Versicherungsmakler begründete Zweifel an der Identität der anfragenden betroffenen Person, dann hat er einen Identitätsnachweis (Ausweiskopie) zu verlangen.

5.3.1. Das Auskunftsrecht

Die betroffene Person ist auf Verlangen über die Verarbeitungszwecke, die Kategorien der Daten die verarbeitet werden, die Empfänger oder Empfängerkategorien, die Speicherdauer, alle verfügbaren Informationen über die Herkunft der Daten (falls die Daten nicht ohnehin beim Betroffenen selbst erhoben worden sind) zu beauskunften.

a. In welcher Form hat der Versicherungsmakler das Auskunftsrecht zu erfüllen?

Der formfreien Geltendmachung des Auskunftsrechts des Betroffenen steht die grundsätzlich formfreie Erfüllung der Ansprüche des Betroffenen durch den Verantwortlichen gegenüber. Allerdings ist dem Versicherungsmakler im eigenen Interesse zu empfehlen, dass er die Erfüllung des Auskunftsanspruchs **schriftlich** dokumentiert (eigenes Beweisinteresse!). Informationen und alle Mitteilungen und Maßnahmen haben kostenlos zu erfolgen.

Aus diesem Grund empfiehlt es sich ein standardisiertes Formular zu erstellen, dass im Anlassfall lediglich individualisiert werden muss.

b. Hat der Versicherungsmakler irgendwelche Fristen zu beachten?

Der Verantwortliche stellt der betroffenen Person Informationen unverzüglich, jedenfalls innerhalb eines Monats nach Eingang der Anfrage zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden (die Frist kann daher insgesamt drei Monate betragen), wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist.

5.3.2. Recht auf Löschung

Die betroffene Person hat das Recht vom Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, diese Daten zu löschen, wenn zB die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind, oder die betroffene Person ihre Einwilligung, auf die sich die Verarbeitung gestützt hat, widerruft, oder die Daten unrechtmäßig verarbeitet wurden (also zB keine Rechtsgrundlage wie Vertrag oder Einwilligung vorliegt).

Dieser Löschungsanspruch besteht nicht, soweit die Verarbeitung (und damit Speicherung) zur Erfüllung einer rechtlichen Verpflichtung notwendig ist, der der Verantwortliche unterliegt. Dies ist für Aufbewahrungs- und Dokumentationspflichten relevant.

5.3.3. Was bedeuten die Betroffenenrechte für den Versicherungsmakler?

Er muss sich Konzepte überlegen, um die Rechte der Betroffenen angemessen und zeitgerecht zu erfüllen.

Weiters ist zu empfehlen, dass sich der Versicherungsmakler standardisierte Vorlagen für eine Beauskunftung bereitstellt, die dann nur noch zu befüllen sind. Wichtig in dem Zusammenhang ist ein ordnungsgemäß und genau geführtes Verarbeitungsverzeichnis, welches bei der Erfüllung der Betroffenenrechte sehr hilfreich sein kann.

To Do's: Standardisiertes Formular zur Erledigung des Auskunftsbegehrens anfertigen. Identitätscheck bei gegründeten Zweifeln.

5.3.4. Welche Auswirkung hat die Verletzung dieser Pflicht?

Die Verletzung der Betroffenenrechte ist mit bis zu EUR 20 Mio oder 4% des letztjährigen weltweiten Jahresumsatzes sanktioniert.

5.4. Was ist die DATA BREACH NOTIFICATION gemäß Art 33 DSGVO?

Als Data Breach wird ein Vorfall verstanden, durch den Unbefugte auf personenbezogene Daten zugreifen (z.B. Verlust eines Datenträgers, Hackerangriff auf die Kundenverwaltungsdatenbank, etc).

Kommt es zu so einem derartigen Vorfall, sind gewisse Melde- und Benachrichtigungspflichten vorgesehen:

1. Meldung an die zuständige Aufsichtsbehörde (= Datenschutzbehörde)

2. Benachrichtigung des Betroffenen

a. Wie und Wann hat die Meldung an die Aufsichtsbehörde zu erfolgen?

Die Meldung einer Datenschutzverletzung an die Aufsichtsbehörde (= Datenschutzbehörde) muss unverzüglich und möglichst binnen 72 Stunden nachdem dem Verantwortlichen diese Verletzung bekannt wurde, erfolgen. Erfolgt die Meldung erst nach Ablauf von 72 Stunden, so ist diese Verzögerung zu begründen.

Die Meldung kann nur dann unterbleiben, wenn die Verletzung nicht zu einem Risiko für die Rechte und Freiheiten der Betroffenen führt. Ob dies der Fall ist sollte der Versicherungsmakler grundsätzlich nicht im Alleingang entscheiden. Die Konsolidierung eines auf das Datenrecht spezialisierten Rechtsanwaltes ist im Falle eines Data Breach jedenfalls anzuraten.

Die Meldung an die Datenschutzbehörde unterliegt grundsätzlich keinen Formvorschriften, muss jedoch bereits eine Beschreibung der Art und des Ausmaßes der Verletzung und auch bereits mögliche Maßnahmen zur Schadenminderung enthalten. Zudem hat der Verantwortliche (Versicherungsmakler) alle Verletzungen zu dokumentieren und diese Dokumentation der Datenschutzbehörde zur Verfügung zu stellen.

b. Wie und wann hat die Benachrichtigung der betroffenen Person zu erfolgen?

Die betroffene Person ist im Falle eines voraussichtlich hohen Risikos für die persönlichen Rechte und Freiheiten unverzüglich von der Datenschutzverletzung zu benachrichtigen. Die Benachrichtigung kann unterbleiben, wenn voraussichtlich kein hohes Risiko zu befürchten ist.

Dem Versicherungsmakler ist grundsätzlich nicht zu empfehlen, diese Prognoseentscheidung (ob ein hohes Risiko besteht) selbst vorzunehmen. Ist er sich hinsichtlich der eigenen Abschätzung nicht sicher, empfiehlt es sich angesichts der vorgesehenen Strafen bei Verletzung der Bestimmungen, jedenfalls die Betroffenen zu benachrichtigen oder sich zumindest von Expertenseite rechtlich absichern zu lassen.

Auch die Benachrichtigung der Betroffenen unterliegt grundsätzlich keinen Formvorschriften. Aus Dokumentationszwecken ist es empfehlenswert, sämtliche Benachrichtigungen schriftlich abzufassen.

c. Welche Folgen hat die Verletzungen gegen die Melde- und Benachrichtigungspflichten

Die Datenschutzbehörde kann Geldbußen in Höhe von bis zu EUR 10 Mio bzw. 2% des Jahresumsatzes. Zudem können Betroffene Schadenersatzansprüche gegen den Verantwortlichen geltend machen, sofern er schuldhaft und kausal gegen die Bestimmungen der DSGVO verstoßen hat.

5.5. Welche MASSNAHMEN zur DATENSICHERHEIT regelt die DSGVO?

Der europäische Gesetzgeber hat sich bei der Erlassung der DSGVO das Ziel gesetzt, die Datensicherheit bei der Verarbeitung personenbezogener Daten in Zukunft noch effektiver zu gewährleisten.

Art 25 DSGVO normiert die Grundsätze des „Datenschutzes durch Technikgestaltung“ (in der englischen Sprachversion und der allgemeinen Diskussion **„Privacy by Design“**) und des „Datenschutzes durch datenschutzfreundliche Technikgestaltung“ (**„Privacy by Default“**).

Sinn und Zweck der Bestimmung ist, den Datenschutz zu einem möglichst frühen Zeitpunkt bei der Auswahl, Festlegung und Einrichtung der Systeme für eine Verarbeitung zu berücksichtigen.

Hersteller oder Produzenten von Systemen sind keine unmittelbaren Adressaten der DSGVO. . Für die Hersteller und Entwickler von Diensten gilt diese Bestimmung lediglich als Appell, datenschutzfreundliche Produkte, Systeme und Dienste anzubieten und einzuführen.

Ein Online-Ratgeber (und weiterführende Informationen) der WKO findet sich auf www.IT-safe.at.

Auf https://wko.at/it-sicherheit finden Sie Infos zu IT-Security mit praktischen Tipps zur Datensicherung und Risikominimierung.

a. Welche Folgen hat die Verletzung der Verpflichtung zur Datensicherheit?

Die Datenschutzbehörde kann Geldbußen in Höhe von bis zu EUR 10 Mio bzw. 2% des Jahresumsatzes. Zudem können Betroffene Schadenersatzansprüche gegen den Verantwortlichen geltend machen, sofern er schuldhaft und kausal gegen die Bestimmungen der DSGVO verstoßen hat.

6. Der Datenschutzbeauftragte

Der Datenschutzbeauftragte soll als interne Kontrollinstanz den Verantwortlichen bzw. den Auftragsverarbeiter bei der Einhaltung des Datenschutzrechts unterstützen.

6.1. Wann muss ein Datenschutzbeauftragter bestellt werden?

Zur Bestellung verpflichtet sind neben Gerichten und Behörden im Wesentlichen alle Privaten, deren Tätigkeit besondere Gefahren für das Persönlichkeitsrecht der von der Datenverarbeitung Betroffenen aufweist.
So ist eine Bestellung verpflichtend vorgesehen, wenn

- die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfanges und/oder ihrer Zwecke eine umfangreiche **regelmäßige und systematische Überwachung** von betroffenen Personen erforderlich machen (z.B. Banken, **Versicherungen**, Kreditauskunfteien und Berufsdetektive).

- die Kerntätigkeit des Unternehmens in der umfangreichen Verarbeitung **sensibler Daten** oder von Daten über **strafrechtliche** Verurteilungen oder Straftaten besteht (z.B. Krankenanstalten).

Es wird in der Regel davon auszugehen sein, dass für den Versicherungsmakler **keine Pflicht** zur Bestellung eines Datenschutzbeauftragten besteht, zumindest solange nicht, als er zB keine personenbezogenen Daten für Profiling-Maßnahmen verarbeitet (dies würde jedenfalls einen Akt der Überwachung im Sinne dieser Bestimmung darstellen) oder seine Kerntätigkeit nicht in der Verarbeitung sensibler Daten (Gesundheitsdaten) besteht.

Eine freiwillige Bestellung ist jederzeit möglich.

7. Datenübermittlung

Wenn eine Datenübermittlung in ein Drittland (außerhalb der EU) stattfindet ist dies nur unter Einhaltung besonderer Bestimmung zulässig. Sofern der Versicherungsmakler also zum Beispiel mit Maklerpartnern, Versicherungskunden oder Versicherern aus Drittländern zusammenarbeitet oder seine Daten an einen Auftragsverarbeiter außerhalb der EU auslagert, ist dies nur zulässig sofern folgende Voraussetzungen erfüllt sind:

- Die Datenübermittlung ist zulässig, wenn das Drittland ein angemessenes Schutzniveau bietet. Die Feststellung des angemessenen Schutzniveaus erfolgt durch die Kommission der EU mittels Angemessenheitsbeschlusses.

- Weiters ist die Datenübermittlung in ein Drittland vorbehaltlich geeigneter Garantien zulässig. Dazu zählen beispielsweise, wenn zwischen Verantwortlichem und in einem Drittland ansässigem Cloud-Anbieter (als Auftragsverarbeiter) eine vertragliche Vereinbarung mit Standarddatenschutzklauseln abgeschlossen wurde oder verbindliche interne Datenschutzvorschriften (Binding Corporate Rules, BCRs), welche von der Aufsichtsbehörde genehmigt wurden, bestehen.
- Zudem ist die Datenübermittlung in ein Drittland zulässig, wenn die betroffene Person in die Datenübermittlung nach Aufklärung über mögliche Risiken ausdrücklich eingewilligt hat.

Ein besonderes Problem in diesem Zusammenhang ist die Inanspruchnahme von Cloud-Services. Denn oftmals werden die Daten innerhalb der Cloud in einem Drittland abgespeichert – die Server der Cloud befinden sich in einem Drittland. Der Versicherungsmakler bleibt auch als Cloud-Nutzer in der Verantwortung der Daten. Erfolgt demnach ein Datentransfer in ein Drittland, muss der Versicherungsmakler überprüfen, welche Bedingungen er und der Empfänger erfüllen müssen, damit Datentransfers rechtmäßig erfolgen. Nach Möglichkeit ist daher anzuraten, Private-Cloud-Anbieter mit Sitz in einem EU-Land auszuwählen.

To Do's: Der Versicherungsmakler muss prüfen ob er Datenübermittlungen in Drittländer vornimmt.

8. Strafen und Rechtsbehelfe im Rahmen der DSGVO

8.1. Welche Geldbußen kann die Behörde verhängen?

Die Möglichkeiten der Behörde general- und spezialpräventiv bei der Verhängung von Geldbußen zu wirken sind exorbitant gestiegen. Frühere „Kavaliersdelikte“ (zB Verletzung des Auskunftsrechts oder des Löschungsrechts: Maximalstrafen von EUR 500) erklärt die DSGVO nun zu mit hohen Bußgeldern belegten Verstößen/Übertretungen:

Für schwerwiegende Verstöße droht eine Geldbuße in Höhe **bis zu 20 Millionen Euro** oder bei Unternehmen **bis zu 4%** des weltweiten Jahresumsatzes des letzten Geschäftsjahres, je nachdem welcher Betrag höher ist.

Für weniger schwere Verstöße droht eine Geldbuße in Höhe **bis zu 10 Millionen Euro** oder bei Unternehmen **bis zu 2%** des weltweiten Jahresumsatzes des letzten Geschäftsjahres, je nachdem, welcher Betrag höher ist.

Bei geringfügigen Verstößen kann die Datenschutzbehörde statt einer Geldbuße auch eine **Verwarnung** aussprechen.

8.2. Welche Rechtsbehelfe hat der Betroffene gegen den Verantwortlichen?

Der Betroffene hat sowohl verwaltungs- als auch zivilrechtliche Rechtsbehelfe gegen den Verantwortlichen. Diese Rechtsbehelfe sind:

- Beschwerderecht an die Datenschutzbehörde
- Klagerecht vor den Zivilgerichten (auch zur Durchsetzung von Schadenersatzansprüchen)
- Beschwerderecht an das Bundesverwaltungsgericht

Wir verbleiben mit freundlichen Grüßen

Christoph Berghammer, MAS
Fachverbandsobmann

Mag. Erwin Gisch, MBA
Fachverbandsgeschäftsführer

Dr. Klaus Koban
Leiter Arbeitskreis Recht