

Vertrag über die Nutzung des SIGNAL IDUNA Extranets für freie Vertriebspartner

zwischen der

SIGNAL IDUNA
Allgemeine Versicherung AG

(nachfolgend SIAV genannt)

und



(nachfolgend Vertriebspartner genannt)

Präambel

Die SIAV betreibt ein über das Internet erreichbares Kunden- und Vertragsdateninformationssystem, das SIGNAL IDUNA Extranet.

Die Kunden- und Vertragsdaten der Vertriebspartner der SIAV sind im SIGNAL IDUNA Extranet abrufbar.

Zu diesem Zweck wird nachfolgender Vertrag geschlossen.

1 Vertragszweck

Das SIGNAL IDUNA Extranet bietet dem Vertriebspartner die Möglichkeit, die für die Betreuung der in seinem Bestand geführten Finanz- und Versicherungsverträge notwendigen Informationen, insbesondere zu Kündigungen und Beitragsrückständen, über eine Internetverbindung abzurufen.

2 Vertragsgegenstand

Der Vertriebspartner erhält das nicht ausschließliche, nicht übertragbare Recht zum Zugang und zur Nutzung des SIGNAL IDUNA Extranets im Rahmen dieser Vereinbarung.

3 Zeitliche Möglichkeit der Nutzung

SIAV ist bemüht, die Datenverbindung zur Nutzung des SIGNAL IDUNA Extranets täglich für 24 Stunden zu ermöglichen und hierfür die technischen Voraussetzungen zu schaffen. Technisch bedingte Nutzungseinschränkungen einzelner Teilsysteme zu bestimmten Tageszeiten werden in den jeweiligen Systemen bekannt gegeben sowie schnellstmöglich behoben. Die Gewähr für eine jederzeitige und sofortige Verfügbarkeit der Datenverbindung sowie des Extranet kann die SIAV nicht übernehmen.

4 Vertraulichkeit und Datenschutz

4.1 Die Parteien verpflichten sich über die Dauer dieses Vertrages hinaus gegenseitig zur vertraulichen Behandlung aller Informationen und Unterlagen, die sie im Rahmen dieses Vertrages von der jeweils anderen Seite erhalten.

4.2 Die bereits als Anlage zur/zum Courtagezusage/Mehrfachagenturvertrag vom Vertriebspartner abgegebene Erklärung Verpflichtung auf die Vertraulichkeit ist auch Bestandteil dieses Vertrages. Der Vertriebspartner trägt insbesondere auch dafür Sorge, dass unbefugten Personen die Nutzung des SIGNAL IDUNA Extranets und die Kenntnisnahme gespeicherter Daten verwehrt ist. Insofern hat er auch Sorge dafür zu tragen, dass die Regelungen der Datenschutzgrundverordnung (DSGVO) und des BDSG bei der Nutzung des SIGNAL IDUNA Extranets beachtet werden. Besondere Aufmerksamkeit ist der Entsorgung von Altpapier sowie der Nutzung bzw. Vernichtung von Daten bzw. Datenträgern, welche über das Portal bezogen wurden, zu widmen.

4.3 Sofern der Vertriebspartner sich zur Erfüllung seiner Aufgaben und Verpflichtungen eigener Mitarbeiter und Hilfspersonen bedient, ist er berechtigt, diesen die Nutzung des SIGNAL IDUNA Extranets zu ermöglichen. Zur Ausübung dieser Tätigkeiten erhalten die Mitarbeiter/Hilfspersonen eigene, auf diese personalisierte, Zugangsdaten. Die Nutzung darf nur zur Erfüllung dieser Aufgaben/Verpflichtungen erfolgen. Die Mitarbeiter/Hilfspersonen sind entsprechend der hier niedergelegten Verpflichtungen zu verpflichten.

Weiter verpflichtet sich der Vertriebspartner, in eigener Verantwortung Mitarbeiter/Hilfspersonen auf die Vertraulichkeit zu verpflichten. Die Mitarbeiter/Hilfspersonen sind im selben Umfang zur Einhaltung der Datenschutzvorschriften verpflichtet, wie der Vertriebspartner selbst. Insofern besteht zwischen den Mitarbeitern/Hilfspersonen und SIAV ein vertragsähnliches Vertrauensverhältnis, während die vertraglichen Beziehungen ausschließlich zwischen Vertriebspartner und den Mitarbeitern/Hilfspersonen bestehen. Die Mitarbeiter/Hilfspersonen sind durch den Vertriebspartner ausdrücklich auf diesen Sachverhalt hinzuweisen.

4.4 Fordert ein Kunde/Interessent Auskunft über Daten, die über seine Person im SIGNAL IDUNA Extranet gespeichert sind, so gibt der Vertriebspartner das Auskunftersuchen unverzüglich der Datenschutz-Organisation der SIGNAL IDUNA Gruppe, Joseph-Scherer-Straße 3, 44139 Dortmund, Tel. 0231/135-0, datenschutz-organisation@signal-iduna.de weiter. Auskünfte werden ausschließlich von der Datenschutz-Organisation der SIGNAL IDUNA Gruppe erteilt.

5 Kostentragung

Die für einen Zugriff auf das SIGNAL IDUNA Extranet notwendige EDV-Ausstattung (Hard- und Software) ist vom Vertriebspartner selbst bereitzustellen. Alle anfallenden Verbindungskosten sind vom Vertriebspartner zu tragen. Die Nutzung des SIGNAL IDUNA Extranet ist für den Vertriebspartner kostenlos.

6 Pflichten des Vertriebspartners

6.1 Die Berechtigung für das SIGNAL IDUNA Extranet erfolgt mittels der von der SIAV zur Verfügung gestellten Zugangsdaten. Diese werden dem Benutzer in Textform zur Verfügung gestellt.

6.2 Der Vertriebspartner ist verpflichtet, die Zugangsdaten gegenüber unbefugten Dritten geheim zu halten. Insbesondere sind Benutzername und Passwort so aufzubewahren, dass der Zugriff auf diese Daten durch unbefugte Dritte unmöglich ist, um einen Missbrauch des Zugangs durch Dritte auszuschließen. Der Vertriebspartner verpflichtet sich, das Passwort unverzüglich zu ändern, sobald er davon Kenntnis erlangt, dass unbefugten Dritten das Passwort bekannt ist.

6.3 Der Vertriebspartner ist verpflichtet, Änderungen hinsichtlich der vergebenen Berechtigungen (z.B. Ausscheiden von Mitarbeitern/Hilfspersonen) unverzüglich der SIAV anzuzeigen, damit die Berechtigungen entsprechend angepasst bzw. gelöscht werden können.

6.4 Der Vertriebspartner ist verpflichtet, seine IT auf einem technisch aktuellen Sicherheitsstand zu halten. Hierzu zählt der Einsatz einer Firewall sowie eines aktuellen Virenschutzprogramms.

6.5 Sollte es bei der Nutzung des SIGNAL IDUNA Extranet zu technischen Störungen kommen, so wird der Vertriebspartner SIAV davon unverzüglich in Kenntnis setzen. Der Vertriebspartner verpflichtet sich darüberhinaus, jeden Verdacht auf Missbrauch, Datenverlust oder unbefugten Zugriff unverzüglich an die SIAV zu melden. Die SIAV behält sich vor, bei sicherheitsrelevanten Vorkommnissen den Zugang zum SIGNAL IDUNA Extranet zu sperren.

6.6 Bei der Übermittlung von Daten aus dem Portal (z. B. in Kundenkorrespondenz) verpflichtet sich der Makler, sichere Kommunikationswege zu verwenden und keine unsicheren Kanäle wie private Messenger oder unverschlüsselte E-Mails zu nutzen.

7 Kontroll- und Nachweispflichten

Der Vertriebspartner verpflichtet sich, der SIGNAL IDUNA auf deren Verlangen Auskunft über die Einhaltung der Bestimmungen zur Datensicherheit gemäß den Ziffern 4 und 6 dieser Vereinbarung zu erteilen. Zu diesem Zweck wird der Vertriebspartner einfache Nachweise (z. B. die Bestätigung der eingesetzten Schutzmaßnahme) erbringen.

8 Pflichten der SIAV

8.1 Soweit die Verfügbarkeit der Datenverbindung und des SIGNAL IDUNA Extranets gewährleistet ist und die SIAV oder eine andere Gesellschaft der SIGNAL IDUNA Gruppe dem Vertriebspartner mitteilt, dass für ihn Bestandsinformationen im SIGNAL IDUNA Extranet zum Abruf bereitgestellt sind, erklärt der Vertriebspartner sein Einverständnis damit, dass er insoweit auf die postalische Zusendung dieser Bestandsinformationen in Papierform verzichtet. Bei längeren Verbindungsunterbrechungen hat der Vertriebspartner in eigener Verantwortung und auf eigene Initiative die für seine Tätigkeit erforderlichen Informationen sowie weitere Informationen, insbesondere zu Kündigungen und Rückstandsinformationen, auf herkömmlichem Weg bei SIAV anzufordern.

8.2 SIAV hat dafür Sorge zu tragen, dass die angebotenen Inhalte stets vollständig und richtig sind sowie aktualisiert und angepasst werden. Sofern mittels Link auf andere Web-Sites verwiesen wird, unterliegen diese Inhalte nicht der Kontrolle der SIAV, so dass diese jede Verantwortung für die Inhalte ablehnt. Sie macht sich diese ausdrücklich nicht zu eigen. Weiter wird darauf hingewiesen, dass Inhalt und Aufbau der Seiten des SIGNAL IDUNA Extranets urheberrechtlich geschützt sind. Die enthaltenen Informationen dürfen daher nur im Rahmen dieses Vertrages oder mit ausdrücklicher Zustimmung der SIAV genutzt und vervielfältigt werden.

9 Haftung

Für den Fall des nicht bestimmungsgemäßen Gebrauchs des SIGNAL IDUNA Extranets durch den Vertriebspartner bzw. seine Mitarbeiter/Hilfspersonen ist die SIAV berechtigt, die Zugangsberechtigung ohne Einhaltung einer Frist vorübergehend oder dauerhaft zu sperren.

10 Vertragsdauer und Kündigung

10.1 Der Nutzungsvertrag beginnt mit dem 08.05.2026.

10.2 Der Nutzungsvertrag kann von den vertragsschließenden Parteien unter Einhaltung einer vierwöchigen Kündigungsfrist zum Ende eines Kalendervierteljahres gekündigt werden. Der Nutzungsvertrag endet ohne ausdrückliche Kündigung mit der Beendigung des Handelsvertretervertrages mit der SIAV bzw. einem Unternehmen der SIGNAL IDUNA Gruppe.

Bei Versicherungsmaklern endet der Nutzungsvertrag ohne ausdrückliche Kündigung bei Widerruf der Courtagezusage nur insoweit, als kein Anspruch auf Zahlung von Folgecourtage mehr besteht.

10.3 Das Recht auf außerordentliche Kündigung aus wichtigem Grund bleibt unberührt. Dies gilt insbesondere im Fall von Ziffer 9.

11 Änderung des Nutzungsvertrages

11.1 Nachträgliche Änderungen bedürfen der Schriftform.

11.2 Sollte eine Bestimmung dieses Vertrages unwirksam, anfechtbar oder undurchführbar sein oder werden, so wird die Gültigkeit des Vertrages im Übrigen nicht berührt. Die Vertragsparteien verpflichten sich bereits jetzt, in einem solchen Fall, die unwirksame, anfechtbare oder undurchführbare Bestimmung durch eine solche zu ersetzen, die dem mit der Bestimmung verfolgten wirtschaftlichen Zweck soweit wie möglich entspricht.

Hamburg, 08.05.2026

SIGNAL IDUNA Allgemeine Versicherung AG

i. V. 

i. V. Andreas Weseloh

i. V. A. Braun-Kell

i. V. Andreas Braun-Kell

Vertriebspartner

Hinweise zur Datensicherheit für Versicherungsmakler und Mehrfachagenten

In Ihrer Funktion als Versicherungsmakler/Mehrfachagent ist der professionelle Umgang mit sensiblen Kundendaten die Grundlage für eine vertrauensvolle und langfristige Kundenbeziehung. Mit den nachfolgenden Informationen bieten wir Ihnen praxisnahe Empfehlungen, um die höchsten Standards der Datensicherheit in Ihrem Arbeitsalltag gewährleisten zu können. Gleichzeitig erfüllen wir die regulatorischen Anforderungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).

1. Stellen Sie eine stabile digitale Infrastruktur sicher

- Zugriffsschutz: Sichern Sie sämtliche Endgeräte (PC, Laptop, Smartphone) durch starke Passwörter, PINs oder biometrische Merkmale, um unbefugte Zugriffe zu verhindern.
- Systemaktualität: Halten Sie Betriebssysteme und Anwendungssoftware durch die regelmäßige Installation von Updates stets auf dem neuesten Stand. Nur so können bekannte Sicherheitslücken effektiv geschlossen werden.
- Schutz vor Schadsoftware: Eine leistungsfähige und permanent aktualisierte Antiviren-Software ist unerlässlich, um Ihre Systeme vor Malware, Ransomware und anderen Bedrohungen zu schützen.

2. Sichern Sie Ihre Kommunikation und Ihren Datentransfer ab

- Phishing-Prävention: Prüfen Sie eingehende E-Mails und deren Anhänge kritisch auf Authentizität. Seien Sie besonders wachsam bei unerwarteten Nachrichten, die dringenden Handlungsbedarf/-verpflichtung, die Bitte um Hilfe suggerieren und/oder verdächtige Links enthalten.
- Autorisierte Kanäle: Der Transfer von Kundendaten darf ausschließlich über gesicherte und für die geschäftliche Nutzung freigegebene Kanäle erfolgen. Die Verwendung privater Messenger-Dienste (z. B. WhatsApp, Signal) ist für diesen Zweck grundsätzlich nicht zulässig.

3. Etablieren Sie eine Sicherheitsroutine für Ihren Arbeitsplatz

- Sichere Aufbewahrung: Implementieren Sie eine „Clean-Desk-Policy“. Physische Unterlagen mit Kundendaten sollten nach der Bearbeitung stets sicher verwahrt (z. B. in abschließbaren Schränken) und niemals offen zugänglich gelassen werden.
- Datenschutzkonforme Entsorgung: Nicht mehr benötigte Dokumente sind fachgerecht mittels eines Aktenvernichters (empfohlene Sicherheitsstufe P-4 nach DIN 66399) zu vernichten.
- Transport und mobile Arbeit: Vermeiden Sie die Aufbewahrung von Kundenunterlagen an unsicheren Orten, wie beispielsweise in einem Pkw.

4. Beachten Sie das „Need-to-Know“-Prinzip

Die Weitergabe von Kundendaten – auch innerhalb Ihres Unternehmens – muss streng nach dem „Need-to-Know“-Prinzip erfolgen. Stellen Sie sicher, dass Mitarbeiter nur auf jene Daten Zugriff erhalten, die für die Erfüllung ihrer spezifischen Aufgaben zwingend erforderlich sind.

5. Verwenden Sie mobile Speichermedien sicher

- Die Nutzung von USB-Sticks oder externen Festplatten sollte auf das absolut notwendige Minimum reduziert werden.
- Sofern der Einsatz unumgänglich ist, ist eine Verschlüsselung der darauf befindlichen Daten obligatorisch.
- Ausgediente Speichermedien müssen fachgerecht und nachweisbar so vernichtet werden, dass eine Datenwiederherstellung ausgeschlossen ist.

6. So handeln Sie richtig bei Sicherheitsvorfällen

- Meldepflicht: Bei Verlust eines Geräts, einem vermuteten unbefugten Datenzugriff oder nach einem Klick auf einen Phishing-Link informieren Sie bitte unverzüglich die SIGNAL IDUNA Allgemeine Versicherung AG per eMail an informationssicherheit@signal-iduna.de.
- Schadensminimierung: Eine umgehende Meldung ist der entscheidende Schritt, um potenzielle Schäden für Ihre Kunden, Ihr Unternehmen und Sie selbst effektiv zu begrenzen.

Ihr sorgfältiger Umgang mit Kundendaten ist ein wesentliches Qualitätsmerkmal Ihrer professionellen Dienstleistung. Denn der Schutz von Informationen ist die Grundlage für Vertrauen.