

## **Datenschutz-Richtlinie**

**Datenschutzorganisation der**

**DIVAL-GmbH Makler für Versicherungen**

**Kiebitzgrund 7 in 12685 Berlin**

**030/540071-0**

[service@dival.de](mailto:service@dival.de)

### **1.Grundsätze**

Der Schutz personenbezogener Daten ist uns ein wichtiges Anliegen. Deshalb verarbeiten wir die personenbezogenen Daten unserer Mitarbeiter, Kunden sowie Geschäftspartner in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit.

In dieser Datenschutzrichtlinie wird beschrieben, welche Arten von personenbezogenen Daten wir erheben, wie diese Daten genutzt werden, an wen sie übermittelt werden und welche Wahlmöglichkeiten und Rechte betroffene Personen im Zusammenhang mit unserer Verarbeitung der Daten haben. Außerdem beschreiben wir, mit welchen Maßnahmen wir die Sicherheit der Daten gewährleisten und wie betroffene Personen Kontakt mit uns aufnehmen können, wenn Sie Fragen zu unserer Datenschutzpraxis haben.

Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die insoweit bei der DIVAL GmbH bestehenden Verantwortlichkeiten. Sie richtet sich an alle Mitarbeiter, die wiederum zur Einhaltung der Richtlinie verpflichtet sind. Adressat sind auch unsere Kunden, Interessenten, Versicherer und Dienstleister.

### **2 Begriffsdefinitionen (Art. 4 DS-GVO)**

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer natürlichen Person (Betroffener). Beispiele: Name, Vorname, Geburtstag, Adressdaten, Vertragsdaten, E-Mail-Inhalte.

Besondere personenbezogene Daten sind Angaben über rassische, ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, sowie wirtschaftliche Verhältnisse.

Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

### **3.Datenschutzbeauftragter (DSB) nach Maßgabe der Art. 37 - 39 DS-GVO/ § 38 BDSGneu:**

Herr Rene' Rautenberg  
Rene' Rautenberg GmbH

Radlkoferstr.2 in 81373 München  
089/55294870  
089/55294879 Fax

Für alle Fragen zum Datenschutz, fragen Sie bitte unseren Datenschutzkoordinator des Unternehmens:

Kristin Höselbarth  
[kh@dival.de](mailto:kh@dival.de)  
030/540071-45

Bitte richten Sie alle Fragen an den Datenschutzkoordinator. Ausnahme: Die Informationen sollen vertraulich behandelt werden. In dem Fall kontaktieren Sie den Datenschutzbeauftragten direkt per Email

Der DSB nimmt die ihm kraft Gesetzes zugewiesenen Aufgaben bei weisungsfreier Anwendung seines Fachwissens sowie seiner beruflichen Qualifikation wahr.

Der Datenschutzbeauftragte unterrichtet und berät die Unternehmensleitung sowie die Beschäftigten hinsichtlich ihrer Datenschutzpflichten. Dafür hat der Datenschutzbeauftragte ein Online Datenschutz Management System zur Verfügung gestellt. Ihm obliegt die Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten der Sensibilisierung und Schulung der Mitarbeiter.

Im Falle risikoreicher Datenverarbeitungen steht der DSB dem Verantwortlichen beratend bei der Abschätzung des Risikos zur Seite.

Der DSB berichtet unmittelbar der Unternehmensleitung. Der DSB hat eine Datenschutz Management Plattform entwickelt. Alle relevanten Datenschutzpunkte sind dort hinterlegt. Die Geschäftsleitung kann jederzeit auf die Informationen zugreifen.

Der DSB wird frühzeitig in alle Datenschutzfragen eingebunden und wird sowohl von der Unternehmensleitung als auch den Beschäftigten bei der Erfüllung seiner Aufgaben unterstützt. Der Datenschutzkoordinator und der DSB ist rechtzeitig einzubinden und zu informieren.

Der Datenschutzk

ordinator ist also insoweit ein dem DSB fachlich zugewiesener Mitarbeiter zur Einhaltung der für das Unternehmen geltenden Datenschutz Vorschriften. Er informiert den DSB über vor Ort aufgetretene Datenschutzfragen. Er erhebt die Angaben über in seinem Zuständigkeitsbereich gesondert eingesetzte Verfahren und gibt die Meldung an den DSB weiter.

Die Unternehmensleitung überträgt die Aufgabe des Führens eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DS-GVO) und des Erteilens von Auskünften (Art. 15 DS-GVO) auf den Datenschutzkoordinator. Für Meldungen, Auskünfte etc. gegenüber den Datenschutzaufsichtsbehörden liegt die bearbeitende Zuständigkeit bei dem Datenschutzkoordinator. Die Fachabteilungen stellen die hierfür erforderlichen

Informationen, Unterlagen etc. zur Verfügung. Gleiches gilt für Anfragen, Beschwerden oder Auskunftsersuchen Betroffener.

Jeder Mitarbeiter kann sich unmittelbar mit Hinweisen, Anregungen oder Beschwerden an den Datenschutzkoordinator wenden, wobei auf Wunsch absolute Vertraulichkeit gewahrt wird.

Der Datenschutzkoordinator berichtet jährlich in einem Tätigkeitsbericht der Geschäftsführung über stattgefundene Prüfungen, Beanstandungen und ggf. noch zu beseitigende Organisationsmängel.

#### **4 Erheben, Verarbeiten und Speichern/Löschung personenbezogener Daten (Art.5 + 6 DS-GVO)**

Das Erheben, Verarbeiten und Speichern personenbezogener Daten in unserem Unternehmen darf nur im Rahmen des rechtlich Zulässigen erfolgen und geschieht auf Basis des von uns verwendeten Maklervertrags oder der Einzelbeauftragung und den mitgeltenden Dokumenten (wie z.B. Vollmacht, Einwilligung zur Datenverarbeitung, die separat unterzeichnet werden). Ohne eine konkrete Beauftragung und eine datenschutzrechtliche Einwilligungserklärung durch unsere Kunden werden wir nicht tätig (bei Kindern und Jugendlichen, die das 16 Lebensjahr noch nicht vollendet haben wird die Einwilligung durch die Erziehungsberechtigten erteilt). Wir dokumentieren unsere Tätigkeit umfangreich über unser Maklerverwaltungsprogramm und halten konkrete Verfahrensanweisungen für die Ausführung unserer Aufträge vor.

Es wird sichergestellt, dass Kunden keiner Entscheidung unterworfen werden, die ausschließlich auf einer automatisierten Verarbeitung beruhen und zugleich den Betroffenen gegenüber eine rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen (bspw. Profiling).

Eine Datenübermittlung findet im Rahmen der Erfüllung unserer vertraglichen Verpflichtung gegenüber dem Mandanten statt um den gewünschten Versicherungsschutz einzudecken und unseren Betreuungspflichten nachzukommen. Empfänger sind insbesondere Versicherer, Dienstleister und von Berufs wegen zur Verschwiegenheit verpflichtete Personen. Eine Übersicht über unsere Geschäftspartner händigen wir auf Wunsch aus.

Falls andere Stellen Informationen über unsere Kunden anfordern, dürfen diese ohne Einwilligung des Betroffenen nur gegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes Interesse des Unternehmens besteht und die Identität des Anfragenden zweifelsfrei feststeht. Im Zweifel ist der Datenschutzkoordinator zu kontaktieren. Eine Übermittlung in Drittländer ist zum aktuellen Zeitpunkt nicht geplant.

Werden externe Dienstleister mit der Verarbeitung personenbezogener Daten bzw. einzelnen Verarbeitungsschritten im Rahmen unserer Vermittlungstätigkeit betraut bzw. mit Tätigkeiten

(z.B. Wartung, Reparatur) beauftragt, bei denen sie die Möglichkeit der Kenntnis personenbezogener Daten bekommen, so wird vor der Beauftragung ein Vertrag zur Auftragsverarbeitung gem. Art. 28 DS-GVO mit diesen abgeschlossen. Durch den Datenschutzkoordinator wird sichergestellt, dass den gesetzlich obliegenden Kontrollpflichten gegenüber dem Auftragnehmer jährlich nachgekommen wird.

Die Speicherung von Daten erfolgt grundsätzlich in unserem Maklerverwaltungsprogramm und auf den zur Verfügung gestellten Netzlaufwerken. Alle Netzwerke laufen über unseren Server. Eine Speicherung auf mobilen Datenträgern oder Cloudspeicher (z.B. Flashspeicher, Streamer-Bändern) erfolgt nur im Rahmen der ausgelagerten Datensicherung durch den Systemadministrator oder seiner Vertretung. Für die Sicherung der Daten im Netzwerk, die auf dem Server gespeichert sind, ist der Systemadministrator verantwortlich.

Die Daten unserer Kunden werden nach Kündigung des Maklervertrages bzw. der Einzelbevollmächtigung nach den gesetzlichen Vorgaben, insbesondere der Bestimmungen zu gesetzlichen Aufbewahrungsfristen gelöscht. Die Fristen können zur Verteidigung von möglichen Rechtsansprüchen entsprechend verlängert werden. An Stelle der Löschung tritt die Einschränkung der Verarbeitung durch Sperrung der Daten.

Gesetzliche Aufbewahrungsfristen und Löschung-/Sperrtermine sind von dem über die Verarbeitung der Daten Entscheidenden in seiner Verantwortung zu beachten. Die jeweils Verantwortlichen in den Arbeitsbereichen sind benannt und in ihre Aufgabe eingewiesen.

Bei der Weiter- oder Rückgabe nicht mehr benötigter IT-Komponenten ist durch den Systemadministrator dafür zu sorgen, dass zuvor sämtliche Daten wirksam gelöscht wurden.

## **5.Sicherheit der Verarbeitung/ Umsetzung technischer und organisatorischer Maßnahmen**

Wir ergreifen alle uns möglichen Maßnahmen, die nach dem aktuellen Stand der Technik, sowie organisatorisch dazu geeignet sind, um Unbefugten keinen Zugriff auf die bei uns gespeicherten personenbezogenen Daten zu gewähren. Bereits bei der Auswahl von Hard- und Software wird das Prinzip der Gewährleistung von Datenschutz durch Technikgestaltung und durch „datenschutzfreundliche“ Voreinstellungen als ein tragendes Kriterium beachtet. Private Hard- und Software dürfen nicht zur Verarbeitung personenbezogener Daten Verwendung finden.

Wir sichern **Vertraulichkeit** durch

- Verpflichtung und Schulung der Mitarbeiter. Alle Mitarbeiter werden bei der Aufnahme ihrer Tätigkeit zur Verschwiegenheit und der Einhaltung der Arbeitsanweisungen sowie dieser Richtlinie verpflichtet. Die Verpflichtung wird jährlich erneuert und der Nachweis in der Personalakte hinterlegt. Die Verpflichtung besteht auch nach der Beendigung ihrer Tätigkeit fort. Der Datenschutzkoordinator

organisiert in Abstimmung mit der Geschäftsleitung jährliche Schulungen zu allen Datenschutz relevanten Themen.

- Verpflichtung Dritter zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes, soweit sie im Rahmen ihrer Tätigkeit z.B. als Handwerker möglicherweise mit personenbezogenen Daten in Kontakt kommen. Es wird sichergestellt, dass ohne Vertraulichkeitserklärung kein Zugang zum nichtöffentlichen Bereich der Firma möglich ist.
- Zutrittskontrolle, indem Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird.
- Zugangskontrolle, indem verhindert wird, dass Unbefugte Datenverarbeitungssysteme nutzen können.
- Zugriffskontrolle, indem wir sichern, dass nur Berechtigte die Datenverarbeitungssysteme nutzen können und dabei auch nur auf die Daten Zugriff haben, für die eine Berechtigung besteht.
- den Einsatz von Aktenvernichtern für personenbezogene Daten, die auf Papier erfasst sind und die sichere Aufbewahrung der Datenträger.
- Einhaltung einer Trennungskontrolle. Es erfolgt eine logische Mandantentrennung durch das Maklerverwaltungsprogramm bei gleichzeitiger Festlegung von Datenbankrechten für dieses und für die Netzlaufwerke.
- Verzicht auf eine Pseudonymisierung der Daten, Profilbildung oder anderer vergleichbarer Auswertungen.
- Verschlüsselung unserer Mails über TLS , was über unseren Anbieter 1&1 erfolgt. Bei Arbeit aus dem Homeoffice wird über die Internetverbindung per Desktop - Virtualisierung (VDI) auf die Daten zugegriffen. Es greift die SSL-Verschlüsselung.

Wir sichern **Integrität** durch

- Kontrolle darüber, dass personenbezogene Daten bei der elektronischen Übertragung, während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, geändert oder entfernt werden.
- Dokumentation der Weitergabe von Daten im Maklerverwaltungsprogramm und Sicherstellung, dass die Mitarbeiter, sich über die Identität des Empfängers von Daten durch geeignete Maßnahmen Gewissheit verschaffen.
- Hinterlegung von Einzelfaxnachweisen und Eingabebestätigungen bei Onlineformularen im Vorgangsticket innerhalb des Maklerverwaltungsprogramms.
- Eingabekontrolle, indem festgestellt werden kann, ob und von wem personenbezogene Daten in das Maklerverwaltungsprogramm eingegeben, verändert oder entfernt wurden. Jeder Mitarbeiter nutzt seinen individuellen Log-In, so dass keine Unbefugten Änderungen oder Löschungen vornehmen können.

Wir sichern **Verfügbarkeit** durch

- Datensicherungsmaßnahmen, die sichern, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden. Alle Daten sind auf dem Server abgelegt und werden täglich gesichert.

Wir achten darauf, dass mit jedem Dienstleister, der in unserem Auftrag personenbezogene Daten verarbeitet oder in Zusammenhang mit seiner Tätigkeit Einblick und Zugriff auf personenbezogene Daten haben könnte, ein Vertrag zur Auftragsverarbeitung mit eindeutiger Leistungsbeschreibung geschlossen wird. Durch den Datenschutzkoordinator wird sichergestellt, dass den gesetzlich obliegenden Kontrollpflichten gegenüber den Auftragnehmern jährlich nachgekommen wird.

**Über Arbeitsanweisungen** haben wir den Inhalt der sich aus den aufgezeigten Maßnahmen ergebenden Aktivitäten und Verantwortlichkeiten präzisiert und exakt geregelt. Hierzu gehören u.a.:

-Vertraulichkeitserklärung für Mitarbeiter und Dritte

-Sicherheitsrichtlinie/Arbeitsordnung

-IT Sicherheitsrichtlinie

## **6. Transparenz der Datenverarbeitung/Verarbeitungsübersichten (Art. 30 DS-GVO)**

Mittels interner Verfahrensübersichten (Verzeichnis der Verarbeitungstätigkeiten) schaffen wir Transparenz innerhalb des Unternehmens und überprüfen, ob unsere Verfahren besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen und damit einer Vorabkontrolle/ Datenschutz-Folgeabschätzung unterliegen. Es besteht die Verpflichtung, diese Übersichten vorzuhalten für eine Einsichtnahme durch die Behörden. Das Verzeichnis kann jederzeit im Datenschutz Management Tool des Datenschutzbeauftragten eingesehen und heruntergeladen werden. Es besteht die Verpflichtung, diese Übersichten vorzuhalten für eine Einsichtnahme durch die Behörden.

Verantwortlich für die Kontrolle der Aktualität der bestehenden Verfahren und deren ggf. erforderlichen Erweiterung ist der Datenschutzkoordinator in Abstimmung mit der Geschäftsleitung

## **7.Rechte von Betroffenen (Art. 12 -23 DS-GVO)**

Der Betroffene kann Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind. Falls im Arbeitsverhältnis nach dem jeweils anzuwendenden Arbeitsrecht weitergehende Einsichtsrechte in Unterlagen des Arbeitgebers (z.B. Personalakte) vorgesehen sind, so bleiben diese unberührt.

Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.

Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.

Der Betroffene ist berechtigt, die Löschung seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende

schutzwürdige Interessen müssen beachtet werden. An Stelle der Löschung tritt die Einschränkung der Verarbeitung durch Sperrung der Daten.

Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten mit Wirkung auf die Zukunft, das zu berücksichtigen ist, wenn sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse an der Verarbeitung überwiegt. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet.

Der Betroffene hat das Recht auf Datenübertragbarkeit. Das bedeutet das Recht, die personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Freiheiten und Rechte anderer Personen dürfen hierdurch nicht beeinträchtigt werden.

Macht ein Betroffener von seinem Auskunftsrecht nach Art. 15 DS-GVO oder seinem Korrektur- oder Widerspruchsrecht nach Art. 16 und Art. 21 DS- GVO Gebrauch, so erfolgt die zentrale Bearbeitung durch den Datenschutzkoordinator.

Der Betroffene hat ein Beschwerderecht bei der Aufsichtsbehörde, in deren Bundesland das Unternehmen seinen Sitz hat. Für unser Unternehmen ist dies:

**Berliner Beauftragte für Datenschutz und Informationsfreiheit  
Friedrichstr. 219 in 10969 Berlin**

## **8.Verfahren bei „Datenpannen“ (Art. 33 DS-GVO)**

Jeder Mitarbeiter ist angewiesen, seinem jeweiligen Vorgesetzten, der Geschäftsführung oder dem Datenschutzkoordinator unverzüglich Fälle von Verstößen gegen diese Datenschutzrichtlinie oder andere Vorschriften zum Schutz personenbezogener Daten (Datenschutzvorfälle) zu melden. Hierzu zählen u.a. Fälle von unrechtmäßiger Übermittlung personenbezogener Daten an Dritte, unrechtmäßiger Zugriff durch Dritte auf personenbezogene Daten oder der Verlust personenbezogener Daten.

Die Geschäftsleitung und der Datenschutzkoordinator prüfen, ob aus dem Vorfall für den oder die Betroffenen ein Risiko zu erwarten ist. Ist dies der Fall, werden in Abstimmung mit dem Datenschutzbeauftragten die Betroffenen persönlich in Kenntnis gesetzt und es erfolgt innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls die Meldung an die zuständige Aufsichtsbehörde (vgl. Ziffer 7).

## **9.Rechenschafts-und Dokumentationspflicht**

Die Einhaltung der Vorgaben, die sich aus dieser Richtlinie ergeben unterliegt einer planmäßigen Kontrolle durch Geschäftsleitung und den Datenschutzkoordinator. Die hierzu realisierten Maßnahmen und Aktivitäten sowie die dazugehörigen Abwägungen werden schriftlich dokumentiert.