Datenschutz- und Datensicherheitsleitlinie

Grundlegende Prinzipien & Werte

Verantwortliche Stelle

AICON Assekuranz und Immobilien GmbH & Co. KG (nachfolgend AICON genannt)
Elbblick 5, 01445 Radebeul
0351/81166-0, info@aicon-makler.de

Bei allen Fragen rund um den Schutz Ihrer Daten erhalten Sie Auskunft durch unsere Geschäftsführung, Sie erreichen uns über die vorgenannten Kontaktdaten. Sie haben Beschwerderecht bei der Aufsichtsbehörde, in deren Bundesland das Unternehmen seinen Sitz hat. Für unser Unternehmen ist dies der:

Sächsische Datenschutzbeauftragte
Kontor am Landtag
Devrientstr. 1, 01067 Dresden
0351/493-5401, saechsdsb@slt.sachsen.de, www.datenschutz.sachsen.de

Eine Datenübermittlung findet an Versicherer und Dienstleister statt, um den von Ihnen gewünschten Versicherungsschutz einzudecken oder eine Finanzierung oder Geldanlage abzuschließen. Des Weiteren an öffentliche Stellen und Institutionen, sofern eine gesetzliche Verpflichtung besteht. Eine Übersicht über die vorgestellten Geschäftspartner händigen wir auf Wunsch aus bzw. können diese auf unserer Homepage www.aicon-makler.de eingesehen werden.

Geltungsbereich

Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die entsprechenden Verantwortlichkeiten beim oben genannten Unternehmen (und seiner/n Niederlassung/en) auf Basis der gesetzlichen Regelungen der Europäischen Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetz (BDSGneu). Alle Mitarbeiter werden bei der Aufnahme ihrer Tätigkeit zur Verschwiegenheit und der Einhaltung dieser Richtlinie verpflichtet. Die Verpflichtung wird jährlich erneuert und besteht auch nach der Beendigung ihrer Tätigkeit fort. Sie richtet sich neben Mitarbeitern auch an Externe, Versicherer und Dienstleister. Diese Leitlinie tritt zum 25.05.2018 in Kraft. Sie gilt, bis sie außer Kraft gesetzt oder durch eine jüngere Fassung ersetzt wird.

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.

Erheben, Verarbeiten und Speichern personenbezogener Daten (Art. 5 & 6 DSGVO)

Der Umgang mit personenbezogenen Daten ist im bundesdeutschen Datenschutzrecht und in der DSGVO als Verbot mit Erlaubnisvorbehalt geregelt. Damit ist das Erheben, Verarbeiten, Übermitteln und Nutzen von personenbezogenen Daten grundsätzlich verboten. Eine Ausnahme ergibt sich nur, wenn ein Gesetz oder eine andere Rechtsverordnung dies erlaubt oder der Betroffene einwilligt. Das Erheben, Verarbeiten und Speichern personenbezogener Daten in unserem Unternehmen geschieht auf Basis des von uns verwendeten Maklerauftrages und den mitgeltenden Dokumenten (z.B. Maklervollmacht, Einwilligung zur Datenverarbeitung, etc.), die separat unterzeichnet werden. Ohne eine konkrete Beauftragung und eine datenschutzrechtliche Einwilligungserklärung durch unsere Kunden werden wir nicht tätig (bei Kindern und Jugendlichen wird die Einwilligung durch die Erziehungsberechtigten erteilt).

Wir dokumentieren unsere Tätigkeit umfänglich über unser Maklerverwaltungsprogramm und halten konkrete Verfahrensanweisungen für die Ausführung unserer Aufträge vor. Profiling findet in unserem Unternehmen nicht statt. Die Daten werden ausschließlich zu den vereinbarten Zwecken verarbeitet. Die Daten unserer Kunden werden nach Kündigung des Maklervertrages 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.

Leitsätze & Prinzipien

Die AICON schützt die personenbezogenen oder sonstigen vertraulich zu behandelnden Daten ihrer Kundinnen und Kunden, Produktgeber sowie ihrer Beschäftigten und Mitarbeiter. Die Gewährleistung von Datenschutz und Datensicherheit ist Aufgabe und Verpflichtung für alle Beschäftigten. Die Mitarbeiter/innen sind als Nutzer von IT-Systemen bei der Verarbeitung von Daten verpflichtet, diese Leitlinie und die daraus abgeleiteten Standards und Richtlinien – insb. der IT-Sicherheitsrichtlinie – zu beachten. Die Führungskräfte sind für die Einhaltung eines angemessenen Sicherheitsstandards im Datenschutz und in der Datensicherheit verantwortlich. Dabei gelten folgende Grundsätze:

- **Prinzip der Datenvermeidung:** Hieraus leitet die AICON ab, für alle ihre Arbeitsvorgänge die Erhebung, Verarbeitung, Übermittlung und Nutzung von personenbezogenen Daten soweit möglich zu vermeiden.
- **Prinzip der Erforderlichkeit:** Soweit bei Arbeitsvorgängen die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nicht vermieden werden kann, wählt die AICON im Rahmen des technisch Vertretbaren jeweils den Arbeitsvorgang, bei dem so wenig personenbezogene Daten wie möglich erhoben, verarbeitet, übermittelt und genutzt werden müssen.
- **Prinzip der Zweckbindung:** Eine Verwendung von personenbezogenen Daten für einen anderen als den vorab festgelegten Zweck ist ausgeschlossen, es sei denn es liegt eine Einwilligung des Betroffenen vor oder ein Gesetz bzw. eine Rechtsvorschrift erlaubt oder ordnet dies an.
- **Prinzip der Datensparsamkeit:** Bei allen Arbeitsvorgängen werden die gesetzlichen Löschfristen beachtet. Werden personenbezogene Daten nicht mehr benötigt, werden sie ohne Ausschöpfung der Löschfristen vorzeitig gelöscht.
- **IT-Sicherheit:** Eine wirksame Umsetzung des Datenschutzes ist nur mit einer wirkungsvollen IT-Sicherheit zu erreichen. Entsprechend formuliert die AICON neben den Prinzipien zur Umsetzung des Datenschutzes auch Prinzipien zur IT-Sicherheit und eine daraus resultierende IT-Sicherheitsrichtlinie.
- **weitere geltende Grundsätze:** Wahrung der Persönlichkeitsrechte, Transparenz, sachliche Richtigkeit & Aktualität der Daten, Vertraulichkeit & Sicherheit bei der Datenverarbeitung

Die unberechtigte Einsichtnahme oder Weitergabe von Daten der AICON ist nicht zulässig. Um den Anforderungen an den Schutz sensibler Daten zu entsprechen, werden die Daten und informationstechnischen Infrastrukturen in ihrer Vertraulichkeit gesichert und alle Mitarbeiter in ihrer Nutzung und Funktion eingewiesen und geschult.

Umsetzung

Die Umsetzung des Datenschutzes und der IT-Sicherheit in den Arbeitsabläufen der AICON erfordert technische und organisatorische 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. Dazu führen wir separate Aufzeichnungen, um die Anforderungen an die Sicherheit der Datenverarbeitung zu dokumentieren.

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.

Sämtliche für unsere Arbeitsabläufe notwendige Hardware (Rechner, Bildschirme, Tastatur, Maus und Peripheriegeräte wie Scanner oder Drucker) wird nach internen Richtlinien gesteuert. Die Rechner werden für die Mitarbeiter bereits konfiguriert und mit den entsprechenden Programmen, die wir im Standard nutzen, ausgestattet. Weitere Software darf nur in Absprache mit der Geschäftsführung installiert werden. Fehlfunktionen und Unregelmäßigkeiten in Daten und informationstechnischen Infrastrukturen sind nur in sehr geringem Umfang und nur in Ausnahmefällen akzeptabel. Daher werden die Daten und informationstechnischen Infrastrukturen der AICON in ihrer Integrität gesichert.

Betroffenenrechte & Verfahren bei Datenpannen (Art. 12 -23 DSGVO & Art. 33 DSGVO)

Jeder Mitarbeiter soll seinem jeweiligen Vorgesetzten, der Geschäftsführung oder dem DSB unverzüglich Fälle von Verstößen gegen diese Datenschutzrichtlinie oder andere Vorschriften zum Schutz personenbezogener Daten (Datenschutzvorfälle) melden. Die verantwortliche Führungskraft ist verpflichtet, den DSB umgehend über Datenschutzvorfälle zu unterrichten. In Fällen von unrechtmäßiger Übermittlung personenbezogener Daten an Dritte, unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten, oder bei Verlust personenbezogener Daten sind die im Unternehmen vorgesehenen Meldungen unverzüglich vorzunehmen, damit nach staatlichem Recht bestehende Meldepflichten von Datenschutzvorfällen erfüllt werden können.
Der von einer Datenschutzpanne Betroffene, hat besondere Rechte, die in einer separaten Erklärung dokumentiert sind.