CYBER CRIME.
BE SAFE!

DER OPTIMALE KOMPLETTSCHUTZ!

CYBER CRIME. VERSICHERUNG.
ANTRAGSMODELL.

Dieses Antragsmodell gilt für Dienstleistungsunternehmen, Selbstständige, freie Berufe (Rechtsanwälte, Steuerberater, Ärzte), Ziviltechniker, Gesundheits- und Heilwesen, Handel, Bildungseinrichtungen, Gastronomie, Hotelerie, Vereine, Verbände, Baugewerbe, Handwerk, Transport, Logistik sowie Land- und Forstwirtschaftsbetriebe.

MARKEL ÖSTERREICH VERSION 10/2024

CYBER CRIME. VERSICHERUNG.
BE SAFE!

BE SAFE!

CYBER CRIME. VERSICHERUNGSSCHUTZ.

DIE HIGHLIGHTS UNSERES VERSICHERUNGSSCHUTZES

CYBER.

HAFTPFLICHTVERSICHERUNG

Versicherungsschutz besteht für Ansprüche Dritter im Zusammenhang mit:

- Dateninfizierungen, -missbrauch, -beschädigung
- Verletzung von Bestimmungen des Datenschutzes
- **Verstöße gegen Geheimhaltungspflichten**
- Rechtsverletzung durch Weitergabe/Veröffentlichung von Informationen oder Medieninhalten
- **Bußgeldern** von Datenschutzbehörden
- Schmerzensgeld aus Verletzungen der Informationssicherheit
- Unzulässigem Zugriff auf versicherte IT-Systeme
- E-Payment inkl. Vertragsstrafen
- Entschädigung mit Strafcharakter
- **Vertragsstrafen**
- **Straf- und Ordnungswidrigkeitsverfahren sowie behördlichen Verfahren**

EIGENSCHADENVERSICHERUNG

Versicherungsschutz für eigene Schäden und Kosten:

- Verletzungen der Informationssicherheit
- Datenmissbrauch und -beschädigung
- fehlerhafte Bedienung und **unvorhergesehene Ausfälle des Computersystems**
- Anordnungen von Datenschutzbehörden
- **Vertragsstrafen**
- **Sachschäden an der Hardware**
- **Beweislastumkehr**

Abhängig vom jeweiligen Vorfall werden unter anderem Kosten übernommen im Zusammenhang mit:

- dem Krisenmanagement
- Benachrichtigungspflichten bei Informationssicherheitsverletzungen
- **Kosten einer freiwilligen Anzeige**
- Internen Untersuchungen
- Computer-Forensik
- **Betriebsunterbrechung:** Ertragsausfall und entgangener Betriebsgewinn für bis zu 180 Tage
- der Wiederherstellung von Daten und des Computersystems
- Kreditüberwachungsdienstleistungen
- Sicherheitsanalysen und **Sicherheitsverbesserungen** inkl. Übernahme der **Kosten** für die **Durchführung** der empfohlenen Maßnahmen
- Public-Relation Maßnahmen

CRIME.

VERTRAUENSSCHADENVERSICHERUNG

Versicherungsschutz besteht für unmittelbare Schäden durch Dritte oder kriminelle Mitarbeiter aufgrund von vorsätzlichen unerlaubten Handlungen, die zum Schadenersatz verpflichten, insbesondere alle Vermögensdelikte wie:

- Diebstahl, Raub, Unterschlagung
- Betrug, Untreue
- **fake president fraud**

In diesem Zusammenhang besteht auch Versicherungsschutz bei

- **Geheimnisverrat inkl.** dem daraus resultierenden **entgangenem Gewinn**
- **Vertragsstrafen**
- **Mittelbare Schäden / Schäden bei Dritten**

BE SAFE!

Abhängig vom jeweiligen Vorfall leistet der Versicherer unter anderem:

- den Ersatz des Schadens
- Abwehrkosten
- Rechts- und Strafverfolgungskosten
- Anwalts-, Sachverständigen-, Zeugen- und Gerichtskosten
- Kosten bei Rufschädigung
- Kosten bei Verdacht auf Geheimnisverrat

BE SAFE!

CYBER CRIME. VERSICHERUNGSSCHUTZ.

SOFORTHILFE – SCHADENBEISPIELE

SOFORTHILFE.

BeforeCrypt
Rufnummer Österreich: +43 800 000183

SOFORTHILFE IM NOTFALL

Unbegrenzter, direkter Zugang zum Krisendienstleister BeforeCrypt GmbH
Der Versicherer übernimmt im Rahmen der vereinbarten Versicherungsbedingungen die Kosten des Krisendienstleisters für eine erste telefonische Notfall- und Krisenunterstützung, **ohne Anrechnung eines Selbstbehaltes.**
Die vereinbarte Versicherungssumme bleibt ebenfalls unberührt.
Hierunter fällt bei Bestehen einer konkreten Risikolage (z. B. Hacker-Angriff, IT-Ausfall, Verschlüsselung von Daten, Datenmissbrauch) Krisenunterstützung in Form von:

- Experteneinschätzung zur geschilderten Lage,
- Empfehlungen für Sofortmaßnahmen zur Schadenbegrenzung,
- Empfehlungen für Sofortmaßnahmen zur Ursachenermittlung
- Bewertung der bisherigen Maßnahmen

SCHADENBEISPIELE.

FAKE PRESIDENT FRAUD: WENN DIE VORTÄUSCHUNG FALSCHER IDENTITÄTEN ZU ZAHLUNGEN AUF EXTERNE KONTEN FÜHRT

Erst ein imitiertes, vertrauliches Schreiben eines angeblich führenden Organs des versicherten Unternehmens, dann die Aufforderung, eine dringende Überweisung auszuführen – so der Trick der Hacker beim „Fake President Fraud", (dt.: „falscher Chef"). Eine Masche mit fatalen Folgen: Die Überweisung führt meist auf ausländische Konten, hauptsächlich in Asien und Osteuropa. Fliegt der Betrug auf, sind diese meist leergeräumt – eine Rückholung ist aufgrund der ausländischen Rechtssysteme erheblich erschwert.

DIGITALE ERPRESSUNG – RANSOMWARE

Hackern gelingt es, Zugriff auf die Patientendaten eines Allgemeinmediziners zu erlangen. Nachdem die Datenbank erfolgreich kopiert wurde, schreiben sie dem Praxisinhaber per Mail und drohen mit der Veröffentlichung der Anamnesen – inklusive Vermerk, woher die Daten stammen. Gegen Zahlung einer horrenden Geldsumme via Western Union könnte er die Veröffentlichung verhindern.

BE SAFE!

KONTAKTDATEN **AssPro managerline** • E-Mail: cyber@apml.at • Website: www.cyberversicherung.eu

CYBER CRIME. VERSICHERUNGSANTRAG.

I. VERMITTLERANGABEN

Vermittlernummer:

Vermittlername:

II. WAS IST DIE HAUPTTÄTIGKEIT DES VERSICHERUNGSNEHMERS?

III. ANGABEN ZUM VERSICHERUNGSNEHMER

Name, Rechtsform

Straße, Nr.

PLZ, Ort

IV. BEGINN DES VERTRAGES

Beginn (Tag/Monat):
(Vertrag wird für 3 Jahre abgeschlossen)

Hauptfälligkeit entspricht Beginn, abweichende Hauptfälligkeit (Tag/Monat):

Der Beginn darf **maximal 3 Monate** in der Vergangenheit liegen. Versicherungsschutz besteht frei von bekannten Pflichtverletzungen und Versicherungsfällen.

CYBER CRIME. FRAGEBOGEN.

V. RISIKOFRAGEN

1. FINANZKENNZAHLEN	des letzten Geschäftsjahres	aktuell	
a. Umsatz (max. 25 Mio.)	€	€	
b. Aktueller Umsatzanteil Europa			%
c. Aktueller Umsatzanteil bzgl. E-Commerce			%

2. IST IHR UNTERNEHMEN IN FOLGENDEN RISIKOBEREICHEN TÄTIG?

Der Tätigkeitsbereich des Antragstellers liegt in den folgenden Bereichen:

- Zahlungsabwicklung, -dienstleistung, Inkassodienstleistung
- Glücksspiel, Pornografie, Datensammlung und -speicherung (Hauptgeschäftszweck)
- Ratingagentur, Vermögensverwaltung, Finanzdienstleistung, Direktmarketing
- Anbieter, Vermittler oder Berater von Versicherungen oder Finanzdienstleistungsprodukten
- produzierendes Gewerbe (Unter die Kategorie produzierendes Gewerbe fallen Unternehmen mit automatisierten Fertigungsmaschinen, -anlagen und -straßen. Beispiele sind Hersteller von Spiel- und Sportwaren, KFZ-Zulieferbetriebe und stromproduzierende Kraftwerke).

○ NEIN ○ ja

3. RISIKO-INFORMATIONEN

Der Antragsteller nutzt folgende IT-Sicherheitsvorkehrungen:

- Anti-Virus-Schutz mit aktuellen Virendatenbanken (Hiervon ausgenommen sind die Betriebssysteme von Apple, Unix und Linux)
- Firewalls an allen Übergängen in das Internet für stationäre IT-Systeme
- Regelmäßige (bis € 1.000.000 Umsatz mind. wöchentliche, ab € 1 .000.000 Umsatz mind. tägliche) Datensicherungen auf separierten Systemen oder Datenträgern (z.B. NAS, externe Festplatte, separierter Server)

○ JA ○ nein

4. RISIKO USA / KANADA

Der Antragsteller erwirtschaftet oder erbringt in den USA direkte Umsätze oder Leistungen.

○ NEIN ○ ja

5. KREDITKARTEN

SPEICHERN oder BEARBEITEN Sie über IHRE EIGENE EDV **im Jahr mehr als** 20.000 Kreditkartendaten?

○ NEIN ○ ja

Sofern Sie Kreditkartendaten speichern oder verarbeiten, sind Sie verpflichtet die Standards gemäß PCI DSS (Payment Card Industry Data Security Standard) einzuhalten.

Falls Sie die Standards gemäß PCI DSS nicht einhalten, bitten wir um entsprechende Mitteilung.

6. PERSONENBEZOGENE DATENSÄTZE

Werden mehr als 100.000 personenbezogene Datensätze gespeichert oder verarbeitet?

○ NEIN ○ ja

(Im Rahmen der PII (Persönlich identifizierbare Informationen) gilt ein Datensatz, unabhängig von der Häufigkeit des gespeicherten Datensatzes als 1 Datensatz = Eine Person (Name, Adresse, Ausweisdaten, Steuerdaten, ethnische Herkunft oder ähnliche Angaben nach Art. 9 DSGVO))

Sofern Sie mehr als 100.000 personenbezogene Datensätze speichern oder verarbeiten, geben Sie uns bitte die Anzahl bekannt: _____

7. LÖSEGELD

Haben Sie das beiliegende Dokument "Empfehlung zu IT-Sicherheit" gelesen und zur Kenntnis genommen?

○ JA ○ nein

CYBER CRIME. FRAGEBOGEN.

8. SOCIAL ENGINEERING

Voraussetzung für den Versicherungsschutz ist, dass die nachfolgend geforderten Sicherheitsvorkehrungen vor Abschluss dieses Antrages im Unternehmen eingeführt und kommuniziert wurden.

Gibt es für den Bereich Social Engineering Fraud (Betrügerische Nachrichten, Fake Mails) eine Risikomanagementstrategie im Unternehmen und wurden alle Mitarbeiter im Umgang mit betrügerischen Nachrichten (Fake Mails) informiert und sensibilisiert? (Falls nicht, werden diese in den nächsten sechs Monaten verbindlich umgesetzt?)	○ JA	○ nein
Werden ungewöhnliche Zahlungsanweisungen, die vorgeblich von Unternehmensleitern / Vorgesetzten erteilt wurden, unter Verwendung der üblichen bekannten Telefonnummern rückbestätigt und auf Authentizität überprüft?	○ JA	○ nein
Werden Anfragen zur Verifizierung von Bankdaten / zum Erhalt von Informationen über Bankkonten, die vorgeblich von Bankangestellten kommen, mit Unternehmensleitern / Vorgesetzten besprochen und wird die Authentizität solcher Anfragen unter Verwendung der bekannten Banktelefonnummer bestätigt?	○ JA	○ nein
Werden Anweisungen zur Änderung von Bankdaten, die vorgeblich von Lieferanten oder Anbietern erteilt wurden, unter Verwendung der bekannten Telefonnummern rückbestätigt und auf Authentizität überprüft und ist immer die Genehmigung eines Vorgesetzten erforderlich?	○ JA	○ nein
Wird das Vieraugenprinzip bei Prüfung der Kontoauszüge eingehalten?	○ JA	○ nein

9. SCHADENERFAHRUNG / UMSTANDSMELDUNGEN

Haben sich in den letzten fünf Jahren behördliche Maßnahmen gegen Ihr Unternehmen gerichtet, die im Zusammenhang mit Ihren IT- bzw. Cyberrisiken stehen?	○ NEIN	○ ja
Wurde in den letzten fünf Jahren bzw. wird gegen Ihr Unternehmen wegen der Verletzung nationalen oder internationalen IT-Rechts (Dateninfizierungen, Verletzungen von Bestimmungen des Datenschutzes, Verstöße gegen Geheimhaltungspflichten, Rufschädigung, Verletzungen von Persönlichkeitsrechten, Markenrechten oder anderen Formen geistigen Eigentums oder Verstöße gegen Wettbewerbsrecht) behördlich oder strafrechtlich ermittelt?	○ NEIN	○ ja
Haben Sie Kenntnis von einem Tatbestand, einer Situation, einem Ereignis oder einer Transaktion, der/die möglicherweise zu einem Schaden im Sinne der beantragten Cyber Crime Versicherung führen könnte?	○ NEIN	○ ja
Wurde Ihr Unternehmen in den letzten fünf Jahren Opfer unbefugten Eindringens in die IT, eines Versagens des Betriebes oder eines sonstigen Angriffs auf Ihre IT-Infrastruktur?	○ NEIN	○ ja
Sind in den letzten fünf Jahren in Ihrem Unternehmen Vertrauensschäden (Unterschlagung, Diebstahl, Betrug, Sabotage etc.) aufgedeckt worden?	○ NEIN	○ ja

CYBER CRIME. VERSICHERUNGSANTRAG.

10. ZUSATZFRAGEN FÜR UNTERNEHMEN MIT EINEM JAHRESUMSATZ GRÖSSER ALS € 10 MIO.

Gibt es einen 4-Augen-Freigabeprozess in der Banking-Software für Überweisungen bei Beträge größer als € 10.000?	○ JA	○ nein
Bitte bestätigen Sie, dass Software die vom Hersteller nicht mehr unterstützt wird (Legacy Systeme, z.B. veraltete Betriebssysteme) weder direkt mit dem Internet verbunden ist, noch aus dem Internet auf diese zugegriffen werden kann.	○ JA	○ nein
Wird eine Multifaktor-Authentifizierung (z.B. Authenticator-App) für Fernzugriffe auf das Unternehmensnetzwerk verwendet, auf welchen vertrauliche Firmendaten und personenbezogenen Daten gespeichert sind?	○ JA	○ nein

VI. VERSICHERUNGSSUMMEN UND SELBSTBEHALTE

Die Versicherungssumme steht zweifach im Jahr zur Verfügung. Prämie netto zzgl. 11% Versicherungssteuer

Versicherungssumme	250.000	500.000	750.000	1.000.000
Umsätze in €				
bis 250.000	○ 562	○ 702	○ 815	○ 929
bis 500.000	○ 621	○ 778	○ 902	○ 1.026
bis 1.000.000	○ 751	○ 940	○ 1.091	○ 1.242
bis 1.500.000	○ 902	○ 1.129	○ 1.242	○ 1.350
bis 2.500.000	○ 950	○ 1.253	○ 1.334	○ 1.415
bis 5.000.000	○ 1.026	○ 1.355	○ 1.534	○ 1.706
bis 7.500.000	○ 1.172	○ 1.555	○ 1.863	○ 2.095
bis 10.000.000	○ 1.339	○ 1.798	○ 2.149	○ 2.419
bis 15.000.000	○ 2.176	○ 2.968	○ 3.363	○ 3.957
bis 20.000.000	○ 2.669	○ 3.640	○ 4.126	○ 4.854
bis 25.000.000	○ 3.157	○ 4.305	○ 4.880	○ 5.741

CYBER CRIME. Selbstbehalt und Versicherungsbedingungen

- € 500 je Versicherungsfall
- Bei einer Cyber-Betriebsunterbrechung gilt ein zeitlicher Selbstbehalt von 6 Stunden und eine Haftzeit von 180 Tagen.

Der Selbstbehalt findet **keine** Anwendung bei Kosten im Zusammenhang oder aufgrund von Leistungen bei Soforthilfe im Notfall und bei vorsorglichen Schadenmeldungen.

Allgemeine Versicherungsbedingungen AVB Österreich Version 10/2024

CYBER CRIME. Versicherungsprämie

Jahresnettoprämie	€	0,00
+ 11% Versicherungssteuer	+ €	0,00
Jahresbruttoprämie	**= €**	0,00

Zahlungsweise: ○ Zahlschein (jährlich) ○ SEPA (beil. Mandatsblatt)

CYBER CRIME. VERSICHERUNGSANTRAG.

VII. RISIKOTRÄGER

Markel Insurance SE
Sopienstraße 26
80333 München
Deutschland

VIII. EXKLUSIVITÄT

Die vorliegende exklusive AssPro Cyber Crime Versicherung ist nicht übertragbar. Im Fall eines Betreuungswechsels von der Asspro managerline auf Dritte kann der Vertrag nicht über den Vertragsablauf hinaus fortgeführt werden. Der Vertrag wird in diesem Fall zum nächstmöglichen ordentlichen Kündigungstermin aufgehoben.

IX. CYBER-PRÄVENTION BASIS (PERSEUS-BASIS)

In Kooperation mit Perseus stellt der Versicherer nachfolgende Trainings und Präventionsmaßnahmen zur Daten- und Cyber-Sicherheit zur Verfügung (Perseus-Basis):

- Einmalige IT-Sicherheitsprüfung,
- Online-Training Cybersicherheit & Datenschutz für maximal 3 Mitarbeiter,
- Einmalige Phishingtest,
- Browser-Check,
- Passwort-Generator,
- Checklisten,

Zugang zu den Trainings- und Präventionsmaßnahmen zu Daten- und Cyber-Sicherheit
https://markel-insurance.at/assistance/
Die Registrierung erfolgt mit der im Versicherungsschein genannten Versicherungsscheinnummer.

X. SCHLUSSERKLÄRUNG

Diese ausgefüllte Erklärung sowie die beigefügten Anlagen werden bei Abschluss eines Vertrages Grundlage und Bestandteil des Versicherungsvertrages. Die Risikoangaben sind vorvertragliche Anzeigen. Hinsichtlich der Folgen bei der Verletzung vorvertraglicher Anzeigepflichten verweisen wir auf die beigefügte Belehrung. Mit Ihrer Unterschrift bestätigen Sie, dass die gemachten Angaben vollständig und richtig sind und dass Sie folgende Dokumente rechtzeitig vor Antragsstellung erhalten und zur Kenntnis genommen haben: AssPro Cyber Crime Bedingungen, Informationspflichten, Belehrung gemäß §§ 16 ff VersVG, Datenschutzhinweis.

Der Unterzeichner bestätigt, dass die in dem Fragebogen abgegebenen Erklärungen und Angaben nach bestem Wissen und Gewissen vollständig und richtig sind und nach Rücksprache mit dem Vorstands- oder Geschäftsführungsgremium oder einer vorhandenen Rechts- oder Versicherungsabteilung beantwortet wurden. Änderungen, die sich nachträglich vor dem Abschluss des Vertrages ergeben, sind dem Versicherer unverzüglich anzuzeigen. Der Unterzeichner weiß, dass seine Angaben Grundlage der Risikobeurteilung des Versicherers sind. Bei Zustandekommen des Vertrages gelten die Angaben als vorvertragliche Angaben im Sinne der §§ 16 ff. Versicherungsvertragsgesetz (VersVG). In Hinsicht auf den Kenntnisstand für die in dem Antrag abgegebenen Erklärungen und Angaben werden keine Angaben bzw. Wissen oder Handlungen, Unterlassungen oder Zusicherungen jeglicher versicherter Personen einer anderen versicherten Person zugerechnet.

Datum	Unterschrift eines Repräsentanten des Unternehmens	Stellung im Unternehmen

EINE VORLÄUFIGE DECKUNG BESTEHT ERST NACH RÜCKBESTÄTIGUNG DURCH ASSPRO!

DRUCKEN | ZURÜCKSETZEN

CYBER CRIME. SEPA-LASTSCHRIFTMANDAT FÜR WIEDERKEHRENDE ZAHLUNGEN.

AssPro managerline GmbH | Augustinusstraße 11c | 50226 Frechen
Gläubiger-Identifikations-Nummer **DE05ZZZ00000073987**

Ich ermächtige / wir ermächtigen die AssPro managerline GmbH, wiederkehrende Zahlungen von meinem / unserem Konto mittels Lastschrift einzuziehen.
Zugleich weise ich / weisen wir mein / unser Kreditinstitut an, die von der AssPro managerline GmbH von meinem / unserem Konto gezogenen Lastschriften einzulösen.

HINWEIS: Ich kann / wir können innerhalb von acht Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrages verlangen. Es gelten dabei die mit meinem / unserem Kreditinstitut vereinbarten Bedingungen.

Versicherungsnehmer

Kontoinhaber – wenn abweichend zum Versicherungsnehmer

Straße, Hausnummer

PLZ, Ort

Bitte unbedingt ausfüllen:

BIC __ __ __ __ __ __ __ __ | __ __ __
8 oder 11 Stellen

IBAN __ __ __ __ | __ __ __ __ | __ __ __ __ | __ __ __ __ | __ __ __ __ | __ __

Zahlungsweise: ○ Jährliche Zahlung ○ Halbjährliche Zahlung (3% Zuschlag)

Jahresbruttoprämie bei jährlicher Zahlung	= €	0,00
Jahresbruttoprämie inklusive 3 % Zuschlag bei halbjährlicher Zahlung	= €	0,00

Im Falle einer Rücklastschrift, die mangels Deckung oder Angabe einer falschen Kontoverbindung erfolgt ist, darf der Zahlungsempfänger dem Zahlungspflichtigen die tatsächlichen Kosten für die Lastschriftrückbuchung im Sinne eines Schadenersatzes in Rechnung stellen.

Datum, Ort und Unterschrift / Firmenstempel des Kontoinhabers

Die Informationen zum Datenschutz gemäß Art. 13 und 14 DSGVO finden Sie unter
https://www.asspromanagerline.at/de/impressum-datenschutz/datenschutzerklaerung.pdf

Markel Insurance SE

Informationsblatt zur CYBER - CRIME - VERSICHERUNG

ACHTUNG:
Hier finden Sie nur ausgewählte Informationen in vereinfachter Form, um Ihnen einen Überblick zu geben. Alle vorvertraglichen und vertraglichen Informationen über das Produkt finden Sie im Versicherungsantrag, in der Versicherungspolizze und in den Versicherungsbedingungen.

Um welche Versicherung handelt es sich: CYBER – CRIME – Versicherung

Was ist versichert?

Die Versicherung umfasst im Rahmen der vereinbarten Versicherungssumme(-n)

Cyberversicherung:

- ✓ Haftpflichtansprüche gegen Versicherte aus Datenschutz-, Vertraulichkeits-, Netzwerksicherheitsverletzungen, rechtswidriger Kommunikation oder aus Vertragsstrafen wegen Verletzung von Datensicherheitsstandards in Form der Prüfung der Haftung, der Erfüllung von gerechtfertigten Haftpflichtansprüchen oder der Übernahme der Kosten der Abwehr unberechtigter Ansprüche
- ✓ Eigenschäden des Versicherungsnehmers aus Betriebsunterbrechungsschäden und den notwendigen Wiederherstellungsaufwand
- ✓ den Ersatz von Kosten aus Datenschutzverfahren des Versicherungsnehmers
- ✓ den Ersatz von Kosten aus Krisenmanagement des Versicherungsnehmers
- ✓ den Ersatz von Kosten aus Datenerpressung

Vertrauensschadenversicherung (Crime):

- ✓ Schäden durch vorsätzlich unerlaubte Handlungen von Mitarbeitern, auch wenn diese Dritten zugefügt wurden und Sie für den von Ihrem Mitarbeiter verursachten Schaden haften.
- ✓ Schäden, die Ihnen von Dritten durch vorsätzlich unerlaubte Handlungen unmittelbar zugefügt wurden, sofern diese Handlungen eine Täuschung beinhalten.
- ✓ Schäden durch Geheimnisverrat

Die Versicherungssummen vereinbaren wir mit Ihnen im Versicherungsvertrag.

Was ist nicht versichert?

Allgemeine Ausschlüsse

- x vorsätzlich und rechtswidrig herbeigeführte Schäden
- x Schäden aufgrund vertraglich übernommener Haftungen
- x Schäden wegen der Verletzung von Patentrechten sowie des Missbrauchs von Patenten, wegen der Verletzung von Betriebs- oder Geschäftsgeheimnissen sowie Vorschriften des Kartellrechts.
- x Schäden aufgrund von oder im Zusammenhang mit Krieg und hoheitlichen Eingriffen, mit Naturgefahren, mit Kernenergie oder radioaktiven Substanzen sowie mit Umweltschäden
- x Schäden aufgrund von oder im Zusammenhang mit jedweder Form von Finanzmarkttransaktionen, Lizenzen, Wertpapierrechtsverstößen
- x Schäden aufgrund oder im Zusammenhang mit Glückspiel
- x Schäden im Zusammenhang mit Personenschäden

Ausschlüsse für die Vertrauensschadenversicherung

- x Schäden die durch fahrlässige Handlungen verursacht werden
- x Mittelbare Schäden
- x Schäden die von Anteilseignern verursacht wurden

Gibt es Deckungsbeschränkungen?

Die Leistungen des Versicherers sind

- ! pro Versicherungsfall begrenzt mit der vereinbarten Versicherungssumme bzw. den vereinbarten Sublimits sowie mit dem vereinbarten Selbstbehalt.
- ! für alle innerhalb eines Versicherungsjahres eingetretenen Versicherungsfälle begrenzt mit der in der Versicherungspolizze vereinbarten Versicherungssumme.

Bei Verletzung der vertraglichen Verpflichtungen Entfällt der Versicherungsschutz ganz oder teilweise.

Darüber hinaus gelten beispielsweise folgende wichtige Deckungsbeschränkungen:

- ! In der Versicherungspolizze angeführte Nachmeldefristen
- ! Internationale Sanktionen und Embargos können die Deckung beschränken

Wo bin ich versichert?

✓ Der Versicherungsschutz besteht weltweit.

Welche Verpflichtungen habe ich?

- Der Versicherer ist vor Abschluss des Vertrages, aber auch während der Laufzeit über das versicherte Risiko vollständig und wahrheitsgemäß zu informieren.
- Die Versicherungsprämien sind fristgerecht zu zahlen.
- Das versicherte Risiko darf nach Abschluss des Versicherungsvertrages nicht erheblich vergrößert oder erweitert werden. Eine dennoch eingetretene Gefahrerhöhung ist dem Versicherer zu melden.
- Dem Versicherer sind Versicherungsfälle oder Schäden, die Geltendmachung von Ansprüchen und die Einleitung eines verwaltungsbehördlichen oder gerichtlichen Strafverfahrens unverzüglich in Textform zu melden. Bei der Feststellung und Erledigung oder Abwehr des Schadens ist mitzuwirken (z.B.: Erteilung von Auskünften und Überlassung von Originalbelegen).
- Es müssen alle Maßnahmen getroffen werden, um den Schaden und dessen Folgen so gering wie möglich zu halten.
- Geltend gemachte Ansprüche dürfen nicht anerkannt werden. Wenn Ansprüche gerichtlich geltend gemacht werden, müssen alle Weisungen des Versicherers befolgt und dem vom Versicherer beauftragten Anwalt Vollmacht erteilt werden.
- Wenn die Versicherungsprämie auf Basis des Umsatzes bemessen wird, ist der Versicherer wahrheitsgemäß zu informieren.

Wann und wie zahle ich?

Die Prämie ist jährlich während der Vertragsdauer und im Vorhinein zu bezahlen. Eine halbjährliche Zahlungsweise und die Zahlungsart (z.B.: Zahlungsanweisung per Zahlschein oder online, SEPA-Mandat) können vereinbart werden.

Wann beginnt und endet die Deckung?

- Der Beginn des Vertrages und der Deckung ist in der Versicherungspolizze angegeben. Voraussetzung ist, dass die Zahlung der ersten Versicherungsprämie rechtzeitig und vollständig erfolgt.
- Der Vertrag und die Deckung enden durch Kündigung durch den Versicherer oder den Kunden.
- Beträgt die vereinbarte Vertragsdauer weniger als 1 Jahr, endet der Vertrag ohne das es einer Kündigung bedarf.

Wie kann ich den Vertrag kündigen?

- Unternehmer können Verträge zum Ende der in der Versicherungspolizze angeführten Vertragslaufzeit mit einer Kündigungsfrist von drei Monaten kündigen.
- Darüber hinaus kann der Vertrag aus weiteren Gründen, z.B. nach Eintritt des Versicherungsfalls, vorzeitig gekündigt werden.

Markel Insurance SE
Sitz der Gesellschaft: Sophienstr. 26, 80333 München
Tel: +49 (0)89 20 50 94-000 / service@markel.de / www.markel.de

Registergericht: Amtsgericht München, HRB 233618
Aufsichtsratsvorsitzender: Andrew Davies, Vorstand: Frederik Wulff (Vorsitzender), Dr. Ulfried Spessert, Matthias Schneider
Aufsichtsbehörde: Bundesanstalt für Finanzdienstleistungsaufsicht, Graurheindorfer Str. 108, 53117 Bonn, www.bafin.de

Legal Entity Identifier (LEI): 39120047HKGRHDVOZ354
Versicherungssteuernummer: 802/V20000028431
Umsatzsteuer-Identifikationsnummer (USt-IdNr.): DE320184742

accenture

Empfehlungen zu IT-Sicherheit (Mindest-) Standards

IT-Sicherheits-Strategie

Umsetzung und Dokumentation einer IT-Sicherheits-Strategie, um alle notwendigen IT-Sicherheits-Anforderungen konkret zu definieren und strategische Anforderungen zu beschreiben.

IT Governance und Organisation

Implementation einer IT-Sicherheitsorganisationsstruktur (Organigramm, RACI Matrix) mit Definition von notwendigen Aufgaben, Rollen und Verantwortlichkeiten (z.B. IT-Sicherheitsbeauftragter, IT Risk Manager, IT Compliance Manager, IT-Sicherheitsgremium) sowie Reporting-strukturen.

Training und Awareness

Ein Schulungskonzept zum Thema IT-Sicherheit sollte im Einklang mit den Sicherheitsrichtlinien erarbeitet und regelmäßig auf Basis von gewonnenen Erkenntnissen aus ua. Informationssicherheits-Vorfällen aktualisiert werden.

IT-Risikomanagement

Die Erstellung einer IT-Risikomanagement-struktur mit Risikomanagementlebenszyklus und -prozess sowie einem Behandlungsplan zur Überwachung und Reporting von IT-Risiken sollte durchgeführt werden.

Benutzer- und Berechtigungsmanagement

Erstellung der notwendigen Prozesse für Benutzer- und Berechtigungsmanagement unter Berücksichtigung von IT-Sicherheitsprinzipien, wie z.B. Aufgabentrennung (Segregation of Duties), geringsten Rechte (Principle of Least Privilege) und “Kenntnis nur bei Bedarf“ (Need to Know).

IT Betriebskontinuitäts-Management und Notfallplanung

Umsetzung angemessener Vorkehrungen, um die Kontinuität und Ordnungsmäßigkeit der IT-unterstützenden Tätigkeiten im Unternehmen zu gewährleisten.

Updates und Sicherheitspatches

Update und Sicherheitspatches sollten zeitnah eingespielt werden. Es wird empfohlen, das Patchmanagement und der dafür notwendige Prozess unter Einbezug jeglicher Software (inkl. Firmware) zu definieren.

Backup / Datensicherungen

Ein Datensicherungskonzept sollte vorhanden und umgesetzt sein. Eine mögliche Manipulation der Sicherungskopien sollte mittels technischer Maßnahmen (z.B. für den Fall einer Ransomeware-Attacke) verhindert werden.

Protokollierung und Überwachung

Festlegung von Prozessen für die regelmäßige Aufzeichnung von Ereignissen in den IT-Systemen (Benutzeraktivitäten, Fehler, Sicherheitsereignis, Administratoraktivitäten, ...) und für die sichere Aufbewahrung der Log- und Protokolldateien zum Schutz vor Manipulation und unerlaubtem Zugriff.

Kommunikationssicherheit

Mobile Datenträger (z.B. Mobilgeräte) sollten entsprechend gesichert, verschlüsselt und mithilfe von Passwörtern geschützt werden. Maßnahmen zum Umgang und zur Entsorgung von Datenträgern sollten definiert sein. Firmenserver sollten mit einer Firewall geschützt sein.

Weiterführende Informationen zum Thema IT-Sicherheit

- Finanzmarktaufsichtsbehörde (FMA) Leitfäden zum Thema IT-Sicherheit https://www.fma.gv.at/fma/fma-leitfaeden/
- Wirtschaftskammer Österreich (WKO) https://www.wko.at/service/innovation-technologie-digitalisierung/it-sicherheit-datensicherheit.html
- IKT-Sicherheitsportal Österreich https://www.onlinesicherheit.gv.at/
- Gesamtverband der Deutschen Versicherungswirtschaft e.V. (Der GDV) https://www.gdv.de/de/themen/schwerpunkte/cybersecurity
- Allianz für Cyber-Sicherheit https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/ErsteSchritte/Erste_Schritte_node.html
- Bundesamt für Sicherheit in der Informationstechnik https://www.bsi.bund.de/DE/Home/home_node.html

Weitere Details - Empfehlungen zu IT-Sicherheit (Mindest-)Standards

IT-Sicherheits-Strategie

Diese sollte diverse strategische Sicherheits-Anforderungen beschreiben, wie zum Beispiel die Steuerung der IT-Sicherheit sowie Definitionen von Grundsatzstrategien zu den Themen der IT-Landschaft, IT-Notfallpläne und Lebenszyklusmanagement. Die IT Sicherheits-Strategie sollte unter Einbindung aller relevanten Stakeholder in regelmäßigen Abständen diskutiert und auf Aktualität sowie Erreichung überprüft werden.

IT Governance und Organisation

Erstellung und Implementierung einer IT-Sicherheitsorganisationsstruktur (Organigramm, RACI Matrix), Definition von notwendigen Aufgaben, Rollen und Verantwortlichkeiten (z.B. IT-Sicherheitsbeauftragter, IT Risk Manager, IT Compliance Manager, IT-Sicherheitsgremium) sowie Reportingstrukturen. Bei der Definition der Aufgaben, Rollen und Verantwortlichkeiten sollte auf Interessenskonflikte geachtet und nach dem Prinzip „Segregation of Duties“ gehandelt werden.

Training und Awareness

Ein Schulungskonzept zum Thema IT-Sicherheit sollte im Einklang mit den Sicherheitsrichtlinien erarbeitet und regelmäßig auf Basis von gewonnenen Erkenntnissen aus ua. Informationssicherheitsvorfällen aktualisiert werden. Hierbei können die Schulungen auf unterschiedlichen Kanälen wie Vorträge, Online Trainings, Selbststudium oder Kampagnen (z.B. Phishing-Nachrichten) durchgeführt werden. Schulungen sind nach dem Schulungskonzept in regelmäßigen Abständen durchzuführen. Empfohlen wird nicht nur die einführende Einschulung rasch nach dem Dienstantritt, sondern auch die regelmäßige Weiterbildung.

IT Risikomanagement

Die Erstellung einer IT-Risikomanagementstruktur mit Risikomanagementlebenszyklus und -prozess sowie einem Behandlungsplan zur Überwachung und Reporting von IT-Risiken sollte durchgeführt werden. IT-Risiken sollten entsprechend analysiert und behandelt werden, um mögliche negative Auswirkungen auf den IT-Betrieb und die operativen Kernprozesse des Unternehmens rechtzeitig zu erkennen und zu beheben. Weiters sollten IT-Risiken in den IT-abhängigen Kernprozessen im unternehmensweiten Risikomanagementprozess entsprechend berücksichtigt werden.

Benutzer- und Berechtigungsmanagement

Erstellung der notwendigen Prozesse für Benutzer- und Berechtigungsmanagement unter Berücksichtigung von IT-Sicherheitsprinzipien, wie z.B. Aufgabentrennung (Segregation of Duties), geringsten Rechte (Principle of Least Privilege) und “Kenntnis nur bei Bedarf“ (Need to Know).

Folgende Punkte sollten ua dabei berücksichtigt werden:

IT-Administrator einrichten, sparsam nutzen und für die tägliche Arbeit einen Zugang mit weit weniger Rechten nutzen

Individuelle Mitarbeiterzugänge einrichten und keine „Sammeluser“ verwenden (eigenen Benutzeraccount mit eigenem Passwort für jeden Mitarbeiter)

Komplexe Passwörter erzwingen (z.B. empfohlen min. 10 Zeichen, Sonderzeichen, Zahlen, Groß- und Kleinschreibung, …)

Die Authentifizierung von Benutzern muss auf sicheren Login Prozeduren basieren. Remote-Zugriffe sollten besonders abgesichert werden, wie zum Beispiel mittels Zwei-Faktor-Authentifizierung

IT Betriebskontinuitäts-Management und Notfallplanung

Umsetzung angemessener Vorkehrungen, um die Kontinuität und Ordnungsmäßigkeit der IT-unterstützenden Tätigkeiten im Unternehmen zu gewährleisten.

Folgende Punkte sollten ua dabei berücksichtigt werden:

- Erstellung eines unternehmensweiten Notfallplans, der alle relevanten Bedrohungsszenarien berücksichtigt und auf Basis einer Risikoanalyse ausgearbeitet wird
- Erarbeitung und Dokumentation der Reaktion auf diese Risiken; Festlegen von Maßnahmen, um den Risiken entgegenwirken zu können (siehe IT Risikomanagement)
- Entwicklung eines operativen Notfallplans unter Berücksichtigung der Szenarien aus der Risikoanalyse sowie Definition der Verantwortlichen für die jeweiligen Notfallszenarien
- Festlegung eines Prozesses zur Durchführung und Dokumentation von regelmäßigen Tests des Notfallplans
- Festlegung eines Prozesses für die laufende Weiterentwicklung des Notfallplans

Updates und Sicherheitspatches

Update und Sicherheitspatches sollten zeitnah eingespielt werden. Es wird empfohlen, das Patchmanagement und der dafür notwendige Prozess unter Einbezug jeglicher Software (inkl. Firmware) zu definieren.

Der Patchmanagement Prozess für IT-Systeme sollte ua beinhalten:

- Dokumentation (Test) von Updates und Patches
- Regelmäßige Überprüfung der Aktualität und Verteilung von Updates und Patches
- Programme (z.B. Antivirus) auf dem neuesten Stand halten
- Automatisierte Benachrichtigungen durch Hersteller einzurichten

Backup / Datensicherungen

Ein regelmäßiges (je öfter Daten gesichert werden, desto besser) Datensicherungskonzept sollte vorhanden und umgesetzt sein. Eine mögliche Manipulation der Sicherungskopien sollte mittels technischer Maßnahmen (z.B. für den Fall einer Ransomeware Attacke) verhindert werden. Sicherungskopien sollten in regelmäßigen Abständen getestet werden.

Protokollierung und Überwachung

Festlegung von Prozessen für die regelmäßige Aufzeichnung von Ereignissen in den IT-Systemen (Benutzeraktivitäten, Fehler, Sicherheitsereignis, Administratoraktivitäten, ...) und für die sichere Aufbewahrung der Log- und Protokolldateien zum Schutz vor Manipulation und unerlaubtem Zugriff.

Kommunikationssicherheit

Mobile Datenträger (z.B. Mobilgeräte) sollten entsprechend gesichert, verschlüsselt und mithilfe von Passwörtern geschützt werden. Maßnahmen zum Umgang und zur Entsorgung von Datenträgern sollten definiert sein. Darüber hinaus sollten die Daten auf Handys oder Laptops aus der Ferne gelöscht werden können. Firmenserver sollten mit einer Firewall geschützt sein. Um unberechtigten Zugriff und Sicherheitsvorfälle im Netzwerk erkennen zu können, sollte eine entsprechende Software und technische Maßnahmen zur Sicherheitsüberwachung (Monitoring, Angriffserkennung, Intrusion Detection, ...) definiert und umgesetzt werden.

ALLGEMEINE DATENSCHUTZERKLÄRUNG

Dies ist unsere allgemeine Datenschutzerklärung und hierin wird erläutert, wie wir personenbezogene Daten nutzen, die wir über Personen erfassen. Für die Nutzung unserer Webseite haben wir eine gesonderte Datenschutzerklärung, die Sie beim Besuch unserer Webseite unter https://markel.de/datenschutzerklaerung aufrufen können.

Die Markel Insurance SE (nachfolgend „Markel“) legt besonderen Wert auf den Schutz Ihrer personenbezogenen Daten. Bevor Sie uns personenbezogene Daten über jemand anders bereitstellen, informieren Sie die jeweilige Person bitte – falls dies den Vertragszwecken nicht entgegen steht, oder diese erheblich gefährdet – über diese Datenschutzerklärung und holen Sie (falls möglich) deren Erlaubnis für die Weitergabe ihrer personenbezogenen Daten an uns ein.

1. Begriffsbestimmungen

Unsere Datenschutzerklärung beruht auf den Begrifflichkeiten, die durch den Europäischen Richtlinien- und Verordnungsgeber bei der Europäischen Datenschutz-Grundverordnung (DSGVO) verwendet wurden. Unsere Datenschutzerklärung soll für unsere Kunden, Geschäftspartner und die Öffentlichkeit gut lesbar und verständlich sein. Um dies zu gewährleisten, möchten wir vorab die wichtigsten verwendeten Begrifflichkeiten erläutern.

Wir verwenden in dieser Datenschutzerklärung unter anderem die folgenden Begriffe:

1.1 Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

1.2 Betroffene Person

Betroffene Person ist jede identifizierte oder identifizierbare natürliche Person, deren personenbezogene Daten von dem für die Verarbeitung Verantwortlichen verarbeitet werden.

1.3 Verarbeitung

Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

1.4 Einschränkung der Verarbeitung

Einschränkung der Verarbeitung ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

1.5 Profiling

Profiling ist jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere, um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

1.6 Pseudonymisierung

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, auf welche die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

1.7 Verantwortlicher oder für die Verarbeitung Verantwortlicher

Verantwortlicher oder für die Verarbeitung Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

1.8 Auftragsverarbeiter

Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

1.9 Empfänger

Empfänger ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger.

1.10 Dritter

Dritter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

1.11 Einwilligung

Einwilligung ist jede von der betroffenen Person freiwillig für den bestimmten Fall in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

2. Verantwortlicher

Markel Insurance SE
Sophienstr. 26
80333 München

3. Name und Anschrift des Datenschutzbeauftragten

Der Datenschutzbeauftragte des für die Verarbeitung Verantwortlichen ist:

Martin Holzhofer
Holzhofer Consulting GmbH
Lochhamer Str. 31
82152 München – Planegg
datenschutzbeauftragter@holzhofer-consulting.de

Jede betroffene Person kann sich jederzeit bei allen Fragen und Anregungen zum Datenschutz direkt an unseren Datenschutzbeauftragten wenden.

4. Datenverarbeitung

Die personenbezogenen Daten, die wir über Sie und andere Personen verarbeiten, sind abhängig vom Verhältnis, in dem Sie mit uns stehen. Auch die Art der Kommunikation zwischen uns und die von uns bereitgestellten Produkte und Dienstleistungen haben Einfluss darauf, wie und ob wir personenbezogene Daten verarbeiten.

Es werden verschiedene Arten personenbezogener Daten gespeichert, je nachdem, ob Sie Versicherungsnehmer oder Anspruchsteller sind, Sie bezüglich unserer Dienstleistungen angefragt haben oder Sie aus einer Versicherungsdeckung gemäß einer Versicherungspolice begünstigt sind, die von einem anderen Versicherungsnehmer abgeschlossen wurde (zum Beispiel, wenn Sie versicherte Person einer „D&O Versicherung“ sind).

Ebenso speichern wir andere personenbezogene Daten in verschiedener Weise, wenn Sie zum Beispiel ein Versicherungsmakler oder ein bestellter Vertreter, ein Zeuge oder eine sonstige Person, mit der wir in Beziehung stehen, sind.

Da wir Versicherungsprodukte, Schadensregulierung, Unterstützung und damit verbundene Dienstleistungen anbieten, umfassen die personenbezogenen Daten, die wir speichern und verarbeiten, abhängig vom Verhältnis, in dem Sie mit uns stehen, unter anderem folgende Arten personenbezogener Daten:

4.1 Kontaktangaben

Name, Adresse, E-Mail und Telefonnummer

4.2 Allgemeine Informationen

Geschlecht, Familienstand, Geburtsdatum und Geburtsort (je nach den Umständen)

4.3 Informationen zu Bildung und Beschäftigung

Bildungsstand, Angaben des Arbeitgebers und bisherige Arbeitsstellen (zum Beispiel bei Bewerbern), Fähigkeiten und Erfahrung, Berufszulassungen, Mitgliedschaften und Zugehörigkeiten

4.4 Versicherungs- und Forderungsinformationen

Policen- und Forderungsnummern, Verhältnis zu Versicherungsnehmer, Versichertem, Anspruchsteller oder einer sonstigen relevanten Person, Datum und Ursache des Vermögensschadens, Verlusts oder Diebstahls, der Verletzung, Behinderung oder des Todes, Tätigkeitsberichte (zum Beispiel Fahrtaufzeichnungen) und sonstige Informationen, die für die Ausstellung der Versicherungspolice und die Prüfung und Begleichung von Forderungen relevant sind. Bei einer Haftpflichtversicherung umfasst dies auch Angaben zu Streitigkeiten, Forderungen und Verfahren, die Sie betreffen.

4.5 Behördliche und sonstige offizielle Identifikationsnummern

Sozialversicherungs- und nationale Versicherungsnummer, Reisepassnummer, Steueridentifikationsnummer, Führerscheinnummer oder eine sonstige behördlich ausgestellte Identifikationsnummer

4.6 Finanzielle Informationen und Bankverbindung

Zahlungskartennummer (Kredit- oder Debitkarte), Bankkontonummer oder eine sonstige Finanzkontonummer und Bankverbindung, Kredithistorie, Kreditreferenzinformationen und Kreditwürdigkeit, Vermögen, Einkommen und sonstige finanzielle Informationen, Konto-Login-Informationen und Passworte für den Zugriff auf das Versicherungs-, Forderungs- und sonstige Konten und die Digitalen Dienste von Markel.

4.7 Sensible Informationen

Informationen über Gesundheitsdaten oder sonstige sensible Informationen wie zum Beispiel religiöse Ansichten, ethnische Zugehörigkeit, politische Ansichten oder sexuelle Orientierung erheben und verarbeiten wir grundsätzlich nicht. Sollte dies ausnahmsweise dennoch einmal der Fall sein, holen wir uns vom Betroffenen zuvor eine ausdrückliche Einwilligung ein.

Wir können jedoch ohne Ihre Einwilligung Informationen über Strafregistereintragungen oder Zivilprozesse einholen (zum Beispiel um Betrug zu verhindern, aufzudecken und zu ermitteln) und geben Informationen zur Aufdeckung, Ermittlung und Verhinderung von Straftaten wie Betrug und Geldwäsche an die ermittelnden Behörden weiter.

4.8 Informationen,

die uns die Bereitstellung unserer Produkte und Dienstleistungen ermöglichen: Standort und Bezeichnung von versichertem Eigentum (zum Beispiel Adresse einer Immobilie, Kfz-Kennzeichen oder Identifikationsnummer), Reisepläne, Alterskategorien der zu versichernden Personen, Angaben über die zu versichernden Risiken, Unfall- und Verlusthistorie und Verlustursache, Position als leitender Angestellter, Geschäftsführer oder Gesellschafter oder sonstige Eigentums- oder Geschäftsführungsinteressen an einer Organisation, frühere Streitigkeiten, Zivil- oder Strafverfahren oder förmliche Untersuchungen, die Sie betreffen, und Informationen über sonstige geführte Versicherungen.

4.9 Ergänzende Informationen aus anderen Quellen

Wir und unsere Dienstleister können die von uns erhobenen personenbezogenen Daten durch Informationen aus anderen Quellen ergänzen (zum Beispiel allgemein verfügbare Informationen von Online-Diensten bei sozialen Medien und sonstige Informationsquellen, externe kommerzielle Informationsquellen und Informationen von unseren Konzernunternehmen und Geschäftspartnern). Wir werden diese ergänzenden Informationen gemäß dem geltenden Recht nutzen (unter anderem werden wir auch Ihre Einwilligung einholen, wenn dies erforderlich ist).

5. Zweck der Datenverarbeitung

Wir nutzen personenbezogene Daten, um unsere Geschäftstätigkeiten auszuführen.

Die Zwecke, für die wir Ihre personenbezogenen Daten oder die von anderen Personen nutzen, sind je nach dem Verhältnis, in dem Sie mit uns stehen, wie der Art von Kommunikationen zwischen uns und der von uns erbrachten Dienstleistungen, unterschiedlich. Personenbezogene Daten werden für andere Zwecke genutzt, wenn Sie ein Versicherungsnehmer sind, als wenn Sie ein Versicherter oder ein Anspruchsteller aus einer Versicherungspolice, ein kommerzieller Versicherungsmakler oder ein bestellter Vertreter, ein Zeuge oder eine sonstige Person, mit der wir in Beziehung stehen, sind.

Die wesentlichen Zwecke, für die wir personenbezogene Daten nutzen, sind:

- mit Ihnen und anderen Personen zu kommunizieren,
- Prüfungen durchzuführen und Entscheidungen zu treffen (automatisiert und nicht automatisiert, auch durch das Profiling von Personen) über: (i) die Bereitstellung und die Bedingungen einer Versicherung und (ii) die Begleichung von Forderungen und die Bereitstellung von Unterstützung und sonstigen Dienstleistungen,
- Versicherungs-, Forderungs- und Unterstützungsdienstleistungen sowie sonstige Produkte und Dienstleistungen bereitzustellen, die wir anbieten, wie Prüfung, Verwaltung, Begleichung von Forderungen und Streitbeilegung,
- Ihre Teilnahmeberechtigung zu prüfen in Bezug auf Zahlungspläne und um Ihre Prämien und sonstigen Zahlungen zu bearbeiten,
- die Qualität unserer Produkte und Dienstleistungen zu verbessern, Mitarbeitertraining bereitzustellen und die Informationssicherheit zu wahren (zum Beispiel können wir zu diesem Zweck Anrufe aufzeichnen und überwachen),
- Straftaten wie Betrug und Geldwäsche zu verhindern, aufzudecken und zu ermitteln und andere kommerzielle Risiken zu analysieren und zu verwalten,
- Forschung und Datenanalysen durchzuführen, wie eine Analyse unseres Kundenstamms und sonstiger Personen, deren personenbezogene Daten wir erheben, um Marktforschung durchzuführen – einschließlich Kundenzufriedenheitsumfragen – und die Risiken zu beurteilen, denen unser Unternehmen ausgesetzt ist, dies jeweils im Einklang mit dem geltenden Recht (einschließlich der Einholung von Einwilligungen, wenn dies erforderlich ist),
- gemäß Ihren angegebenen Präferenzen Marketinginformationen bereitzustellen (Marketinginformationen können Produkte und Dienstleistungen betreffen, die anhand Ihrer angegebenen Präferenzen von unseren externen Partnern angeboten werden). Wir können gemäß Ihren Präferenzen Marketingaktivitäten mithilfe von E-Mails, SMS- und sonstigen Textnachrichten, per Post oder Telefon ausführen,
- Ihnen die Teilnahme an Wettbewerben, Preisausschreibungen und ähnlichen Werbeaktionen zu ermöglichen und diese Aktivitäten zu verwalten. Für diese Aktivitäten gelten zusätzliche Bedingungen, die weitere Informationen darüber enthalten, wie wir Ihre personenbezogenen Daten nutzen und offenlegen, wenn dies hilfreich ist, um Ihnen ein vollständiges Bild darüber wiederzugeben, wie wir personenbezogene Daten erheben und nutzen. Diese Informationen werden wir Ihnen rechtzeitig vor der Teilnahme an solchen Wettbewerben oder zum Beispiel Preisausschreibungen zur Verfügung stellen,
- Ihr Besuchererlebnis zu personalisieren, wenn Sie die Digitalen Dienste von Markel nutzen oder Websites Dritter besuchen, indem wir Ihnen auf Sie abgestimmte Informationen und Werbung anzeigen, Sie gegenüber jedem identifizieren, dem Sie über die Digitalen Dienste von Markel Nachrichten zusenden, und die Veröffentlichung in sozialen Medien erleichtern,
- unsere Geschäftstätigkeiten und unsere IT-Infrastruktur zu verwalten und dies im Einklang mit unseren internen Richtlinien und Verfahren, einschließlich derjenigen in Bezug auf Finanzen und Buchhaltung, Abrechnung und Inkasso, IT-Systembetrieb, Daten- und Website-Hosting, Datenanalysen, Unternehmensfortführung, Verwaltung von Unterlagen, Dokument- und Druckmanagement und Rechnungsprüfung,
- Beschwerden, Feedback und Anfragen zu bearbeiten und Anfragen bezüglich der Einsichtnahme oder Korrektur von Daten oder der Ausübung sonstiger Rechte in Bezug auf personenbezogene Daten zu bearbeiten,
- geltende Gesetze und regulatorische Verpflichtungen einzuhalten (einschließlich Gesetzen und Vorschriften außerhalb des Landes, in dem Sie Ihren Wohnsitz haben), zum Beispiel Gesetze und Vorschriften in Bezug auf die Bekämpfung von Geldwäsche, Sanktionen und die Bekämpfung von Terrorismus, um gerichtlichen Verfahren und gerichtlichen Anordnungen nachzukommen und um Aufforderungen öffentlicher und staatlicher Behörden (einschließlich solcher außerhalb des Landes, in dem sich Ihr Wohnsitz befindet) Folge zu leisten,
- gesetzliche Rechte zu begründen, durchzusetzen und zu verteidigen, um unsere Geschäftstätigkeiten und diejenigen unserer Konzernunternehmen und Geschäftspartner zu schützen und um unsere und Ihre Rechte, Privatsphäre, Sicherheit und unser und Ihr Eigentum sowie die Rechte, Privatsphäre, Sicherheit und das Eigentum unserer Konzernunternehmen und Geschäftspartner oder sonstiger Personen oder Dritter zu schützen, um unsere Bedingungen durchzusetzen und um verfügbare Abhilfemaßnahmen zu verfolgen und unsere Schäden zu begrenzen.

6. Rechtsgrundlagen der Datenverarbeitung

Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn es hierfür eine gesetzliche Grundlage gibt. Die DSGVO sieht in Art. 6 verschiedene Rechtsgrundlagen vor, die sich je nach der Art der erhobenen Daten und dem Zweck ihrer Verarbeitung unterscheiden.

Im Regelfall werden wir auf Basis von Art. 6 Abs. (1) lit. b) DSGVO personenbezogene Daten von Ihnen einholen und verarbeiten, um den Abschluss eines Versicherungsvertrags mit Ihnen vorzubereiten oder einen abgeschlossenen Versicherungsvertrag mit Ihnen abzuwickeln und/oder zu erfüllen. Wenn Sie uns die relevanten personenbezogenen Daten nicht bereitstellen, sind wir unter diesen Umständen möglicherweise nicht in der Lage, Ihnen unsere Produkte oder Dienstleistungen bereitzustellen.

Teilweise müssen wir personenbezogene Daten bei Ihnen einholen und verarbeiten, um geltenden gesetzlichen Anforderungen zu entsprechen. Rechtsgrundlage hierfür bildet dann Art. 6 Abs. (1) lit. c) DSGVO.

In besonderen Fällen ist eine Verarbeitung erhobener Daten auch dazu notwendig, unsere berechtigten Interessen oder die eines Dritten zu wahren, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegend dagegen sprechen. In diesem Fall erfolgt die Datenverarbeitung auf Grundlage von Art. 6 Abs. (1) lit. f) DSGVO.

7. Routinemäßige Löschung und Sperrung personenbezogener Daten

Der für die Verarbeitung Verantwortliche verarbeitet und speichert personenbezogene Daten der betroffenen Person nur für den Zeitraum, der zur Erreichung des Speicherzwecks erforderlich ist oder sofern dies durch den Europäischen Richtlinien- und Verordnungsgeber oder einen anderen Gesetzgeber in Gesetzen oder Vorschriften, welchen der für die Verarbeitung Verantwortliche unterliegt, vorgesehen wurde.

Entfällt der Speicherungszweck oder läuft eine vom Europäischen Richtlinien- und Verordnungsgeber oder einem anderen zuständigen Gesetzgeber vorgeschriebene Speicherfrist aus, werden die personenbezogenen Daten routinemäßig und entsprechend den gesetzlichen Vorschriften gesperrt oder gelöscht.

8. Rechte der betroffenen Person

Sie haben die Möglichkeit, jederzeit von Ihren „Betroffenenrechten“ Gebrauch zu machen:

- Recht auf Auskunft gemäß Art. 15 DSGVO.
- Recht auf Berichtigung gemäß Art. 16 DSGVO.
- Recht auf Löschung gemäß Art. 17 DSGVO.
- Recht auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO.
- Recht auf Datenübertragbarkeit gemäß Art. 20 DSGVO.
- Widerspruchsrecht gemäß Art. 21 DSGVO.

Sofern Sie von Ihren Rechten Gebrauch machen möchten, richten Sie Ihr Anliegen bitte per E-Mail an info@markel.de oder per Briefpost an die in Punkt 1 genannte Anschrift. Daneben haben Sie gemäß Art. 77 Abs. 1 DSGVO ein Recht auf Beschwerde bei einer Aufsichtsbehörde. Weitere Informationen erhalten Sie bei der jeweils für Sie örtlich zuständigen Aufsichtsbehörde.