CYBER CRIME.
BE SAFE!

DER OPTIMALE KOMPLETTSCHUTZ!

CYBER CRIME. VERSICHERUNG.
ANTRAGSMODELL.

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

CYBER CRIME. VERSICHERUNG.
BE SAFE!

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. VERSICHERUNG.
BE SAFE!

BE SAFE!

CYBER CRIME. VERSICHERUNGSANTRAG.

I. VERMITTLERANGABEN

Vermittlernummer: Vermittlername:

II. WAS IST DIE HAUPTTÄTIGKEIT DES VERSICHERUNGSNEHMERS?

Branche

III. ANGABEN ZUM VERSICHERUNGSNEHMER

Name, Rechtsform

Straße, Nr.

PLZ, Ort

IV. FINANZKENNZAHLEN

a. Umsatz (max. € 25 Mio.)	€	
b. Umsatzanteil davon EU, EWR, Schweiz		%
c. Umsatzanteil davon USA und Kanada		%
d. Umsatzanteil davon Rest der Welt		%

V. 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.

VI. RISIKOFRAGEN

1. IST IHR UNTERNEHMEN IN FOLGENDEN RISIKOBEREICHEN TÄTIG?

- Zahlungsabwicklung, -dienstleistung, Inkassodienstleistung
- Glücksspiel, Pornografie, Datensammlung und -speicherung (Hauptgeschäftszweck)
- Klinik, Krankenhaus
- Ratingagentur, Direktmarketing
- öffentliche Unternehmen, Gemeinden
- Versorgungsunternehmen (z.B. Energie, Wasser, Telekommunikation)

○ NEIN ○ ja

2. RISIKO-INFORMATIONEN

Der Antragsteller nutzt folgende IT-Sicherheitsvorkehrungen: ○ JA ○ nein

- 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 Datensicherungen (bis € 1.000.000 Umsatz mindestens wöchentliche, ab € 1 .000.000 Umsatz mindestens tägliche) auf separierten Systemen oder Datenträgern (z.B. NAS, externe Festplatte, separierter Server)

3. RISIKO USA / KANADA

Der Antragsteller speichert personenbezogene Daten von in den USA ansässigen Personen ○ NEIN ○ ja

4. LÖSEGELD

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

5. SCHADENERFAHRUNG / UMSTANDSMELDUNGEN

Hat der Antragsteller in den letzten 5 Jahren Schäden durch Cyber- und Daten-Eigenschäden (z.B. Hacker-Angriff, Erpressung, Schadensoftware) oder Cyber-Drittschäden über EUR 1.500 erlitten? Gab es Vorfälle wie Fake-President-Angriffe oder Vertrauensschäden? Sind Umstände bekannt, die zu einem Schaden oder einer Inanspruchnahme führen könnten? (Warnungen durch Firewalls oder Virenscanner ohne Auswirkungen sind nicht zu berücksichtigen.) ○ NEIN ○ ja

Eine Aufsichtsbehörde, staatliche Stelle oder Verwaltungsbehörde hat Klage gegen den Antragsteller eingereicht, Ermittlungen eingeleitet oder Auskünfte angefordert, was den Umgang mit sensiblen Daten angeht. ○ NEIN ○ ja

6. BEI EINEM UMSATZ GRÖSSER ALS € 10 MIO. IST NACHFOLGENDE RISIKOINFORMATION ZUSÄTZLICH ZU BEANTWORTEN

Der Antragsteller nutzt darüber hinaus folgende Sicherheitsvorkehrungen: ○ JA ○ nein

- Vier-Augen-Prinzip: Überweisungen über € 10.000 werden erst nach einer zusätzlichen Freigabe durchgeführt.
- Sichere Netzwerkinfrastruktur: Kein Zugriff auf veraltete Systeme ohne Hersteller-Sicherheitsupdates (z.B. Windows 7/XP/NT) oder Nutzung eines separaten Netzwerkes für solche Systeme.
- Geschützter Fernzugriff: Fernzugriffe auf Systeme mit vertraulichen Unternehmens und personenbezogenen Daten erfolgt ausschließlich über eine 2-Faktor-Authentifizierung (z.B. Authenticator-App) oder VPN-Tunnel.
- Bei Nutzung von Fertigungsmaschinen: Fertigungsmaschinen sind von externen Netzwerken und dem Unternehmensnetzwerk separiert.

CYBER CRIME. VERSICHERUNGSANTRAG.

VII. VERSICHERUNGSSUMMEN UND SELBSTBEHALTE

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

Versicherungssumme	250.000	500.000	1.000.000	2.000.000
Umsätze in €				
bis 250.000	587	734	971	1.165
bis 500.000	649	813	1.072	1.287
bis 1.000.000	785	982	1.298	1.557
bis 1.500.000	943	1.180	1.411	1.693
bis 2.500.000	993	1.309	1.478	1.774
bis 5.000.000	1.072	1.417	1.783	2.140
bis 7.500.000	1.349	1.625	2.189	2.628
bis 10.000.000	1.399	1.880	2.528	3.034
bis 12.000.000	1.819	2.349	3.160	3.792
bis 15.000.000	2.275	3.101	4.134	4.961
bis 20.000.000	2.728	3.803	5.072	6.085
bis 25.000.000	3.299	4.499	5.999	7.198

CYBER CRIME. Sublimits

Als Gesamtleistungsobergrenze je Versicherungsfall gilt die ausgewiesene Gesamtversicherungssumme. Je Versicherungsfall gelten folgende Leistungen bis zu den genannten Leistungsobergrenzen (Sublimits) als versichert:

Vertrauensschäden	Im Rahmen der Versicherungssumme, max. € 1.000.000
Lösegeld	Im Rahmen der Versicherungssumme, max. € 1.000.000

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 03/2026

CYBER CRIME. Versicherungsprämie

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

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

CYBER CRIME. VERSICHERUNGSANTRAG.

VIII. RISIKOTRÄGER

Markel Insurance SE
Sopienstraße 26
80333 München
Deutschland

IX. 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.

X. CYBER-PRÄVENTION PERSEUS

(sofern im Versicherungsschein vereinbart)

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

- Zertifikatskurse – Cybersicherheit (z. B. Antivirensoftware, Firewall, Updates, 2FA)
- Datenschutz (personenbezogene Daten, Zweckbindung, Datenminimierung)
- Phishing (gefährliche Links, Passwörter, Anhänge, Malware)
- Vertiefende Module
- Ransomware
- Social Media
- Mobiles Arbeiten
- Umgang mit Informationen
- Menschliche Firewall
- Cyber-Notfall
- Schadsoftware
- Verschlüsselungssoftware
- Social Engineering
- Phishing-Simulation & Reporting
- Regelmäßige Phishing-Tests basierend auf aktuellen Angriffstrends
- Sensibilisierung der Mitarbeitenden für Phishing-Gefahren
- Echtzeit-Reporting für Admins zur Sicherheitslage
- Gefahrenwarnungen & Handlungsempfehlungen
- Frühzeitige Warnung bei Cybervorfällen, Sicherheitslücken & Bedrohungen
- E-Mail-Benachrichtigungen über neue Risiken
- Konkrete Handlungsempfehlungen zur Prävention & Reaktion
- Technische Werkzeuge für Cybersicherheit
- Malware-Scanner zur Bedrohungserkennung
- Browser-Check zur Sicherheitsprüfung

Einschluss Cyber Prävention mit einem Prämienzuschlag von 5,5% gewünscht ☐ **JA**

CYBER CRIME. VERSICHERUNGSANTRAG.

XI. 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

CYBERVERSICHERUNG
INFORMATIONSBLATT ZU VERSICHERUNGSPRODUKTEN

Unternehmen: Markel Insurance SE **Produkt: Markel Pro Cyber AT**

ACHTUNG: Hier finden Sie nur die wichtigsten Informationen zu Ihrer Versicherung. Die vollständigen vorvertraglichen und vertraglichen Informationen finden Sie im Versicherungsantrag, im Versicherungsschein und in den Versicherungsbedingungen. Damit Sie umfassend informiert sind, lesen Sie bitte alle Unterlagen durch.

UM WELCHE ART VON VERSICHERUNG HANDELT ES SICH?
CYBERVERSICHERUNG

Was ist versichert?

Die Versicherung umfasst

- ✓ von Versicherten untereinander,
- ✓ die Wiederherstellung oder die Reparatur der IT-Systeme, Programme und elektronischen Daten infolge von Hacker-Eingriffen und -Angriffen sowie bei Infektionen mit Schadsoftware einschließlich Prävention-Assistance, sofortiger Nothilfe und Sicherheitsverbesserungen nach einem Schaden (Cyber- und Dateneigenschaden),
- ✓ bei Vertragsstrafen wegen verzögerter Leistungserbringung
- ✓ sofern nicht abgewählt,
  - ✓ Betriebsunterbrechungsschäden infolge von Hacker-Eingriffen und -Angriffen sowie bei Infektionen mit Schadsoftware einschließlich Cloud-Ausfall und Mehrkosten (Cyber-Betriebsunterbrechung),
  - ✓ Geld- oder Warenforderung durch Dritte infolge von einem Cyber-Vorfall (Cyber-Erpressung),
  - ✓ Vermögensschäden in Form von Vertragsstrafen sowie Gebühren und/oder Kosten für verpflichtende Prüfungen (PCI-Compliance), Fallbehandlungen, Kartenneuausstellung und zum Ausgleich der Betrugsschadenshöhe.
  - ✓ Vertrauensschäden in Form von unmittelbar entstandenen Vermögensschäden durch mitversicherte Personen, durch Dritte oder Täuschungen mit der folge von irrtümlichen Zahlungen oder Lieferungen.
  - ✓ die Erfüllung von gerechtfertigten Schadenersatzverpflichtungen sowie die Kosten der Abwehr unberechtigter Ansprüchen bei Verstößen gegen Cyber-Sicherheit, Datenschutz, Geheimhaltungspflichten, Persönlichkeits- und Markenrechten sowie Wettbewerb und Werbung.

Die Versicherungssumme ist dem Versicherungsvertrag zu entnehmen.

Was ist nicht versichert?

Die Versicherung umfasst, sofern nichts Gegenteiliges vereinbart wurde, keine Schäden

- × wegen vorsätzlich herbeigeführten Schäden und wissentlicher Pflichtverletzung in der Haftpflicht,
- × wegen Erbringung der geschuldeten Leistung und wegen Garantiezusagen,
- × bei Kernenergie und Krieg,
- × bei Glücksspiel,
- × durch Hoheitliche Eingriffe,
- × bei Infrastruktur,
- × bei Finanzmarkttransaktionen,
- × bei Rechtswidrigem Erfassen von Daten,
- × bei Patent- und Kartellrechtsverletzungen.

Gibt es Deckungsbeschränkungen?

! Die Bausteine Cyber-Betriebsunterbrechung, Cyber-Erpressung, Cyber-Zahlungsmittel, Cyber-Vertrauensschaden, Cyber-Haftpflicht und Cyber-Prävention sind abwählbar und gelten bei Abwahl nicht versichert.

! Es kann ein Selbstbehalt vereinbart sein.

Wo bin ich versichert?

✓ Der Versicherungsschutz bezieht sich auf Versicherungsfälle weltweit.

Welche Verpflichtungen habe ich?

– Die Versicherungsprämien sind fristgerecht zu zahlen.

– Der Schadenfall, die Erhebung von Ansprüchen sowie die Einleitung eines verwaltungsbehördlichen oder gerichtlichen Strafverfahrens sind fristgerecht dem Versicherer zu melden. An der Feststellung des Sachverhalts muss beigetragen und der entstandene Schaden möglichst gering gehalten werden.

– Ansprüche des Geschädigten dürfen nicht anerkannt werden. Wenn Ansprüche gerichtlich geltend gemacht werden, sind alle Weisungen des Versicherers zu befolgen. Dem vom Versicherer bestellten Anwalt muss die Vollmacht erteilt werden. Wird die Prämie aufgrund von einer Tarifierungsgrundlage wie zum Beispiel Umsatz, Haushaltssumme, Anzahl der Personen bemessen, errechnet, sind die Daten dem Versicherer wahrheitsgemäß zur Fälligkeit mitzuteilen.

– Risikoänderungen sind dem Versicherer unverzüglich mitzuteilen.

Wann und wie zahle ich?

Die Prämie ist grundsätzlich jährlich im Vorhinein zu zahlen. Eine halb- oder vierteljährlich Zahlungsweise und die Zahlungsart (zum Beispiel SEPA oder Überweisung) sind vertraglich zu vereinbaren.

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, in der wir erläutern, wie wir personenbezogene Daten nutzen, die wir über Personen erfassen. Für die Nutzung unserer Webseite haben wir eine gesonderte Datenschutzerklärung, die Sie unter https://markel.de/datenschutzerklaerung einsehen können.

Die Markel Insurance SE (nachfolgend „Markel") legt besonderen Wert auf den Schutz Ihrer personenbezogenen Daten. Bevor Sie uns personenbezogene Daten über Dritte 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. Definitionen der Begriffe

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 (zum Beispiel Stamm-, Versicherungs- und Finanzdaten beziehungsweise Bankdaten).

1.2 Betroffene Person
Betroffene Person ist jede identifizierte oder identifizierbare natürliche Person, deren personenbezogene Daten von dem für die Verarbeitung Verantwortlichen verarbeitet werden (zum Beispiel Makler, Versicherter, Anspruchsteller beziehungsweise Geschädigter).

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.

Stand AT Version 1.2

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 (zum Beispiel Vermittler, externe Dienstleister, Sachverständige). 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. Name und Kontaktdaten des Verantwortlichen

Verantwortlich für die Verarbeitung Ihrer Daten ist:

Markel Insurance SE
Sophienstr. 26
80333 München

3. Kontaktdaten des Datenschutzbeauftragten

Die Kontaktdaten der Datenschutzbeauftragten von Markel sind wie folgt:
ISiCO GmbH
Am Hamburger Bahnhof 4
10557 Berlin
datenschutz@markel.de

Jede betroffene Person kann sich jederzeit bei allen Fragen und Anregungen zum Datenschutz direkt an unseren Datenschutzbeauftragten wenden. Dieser ist unter obiger postalischer Adresse sowie unter der zuvor angegeben E-Mail-Adresse (Stichwort: „z. Hd. Datenschutzbeauftragter“) erreichbar. Wir weisen ausdrücklich darauf hin, dass bei Nutzung dieser E-Mail-Adresse die Inhalte nicht ausschließlich von unserem Datenschutzbeauftragten zur Kenntnis genommen werden. Wenn Sie vertrauliche Informationen austauschen möchten, bitten wir Sie daher zunächst über diese E-Mail-Adresse um direkte Kontaktaufnahme.

4. Daten, die wir verarbeiten

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 Passwörter 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 Versicherungsrelevante Informationen
Informationen, die uns die Bereitstellung unserer Produkte und Dienstleistungen ermöglichen wie zum Beispiel 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:

- zur Prüfung eines eingetretenen Schadenfalls. Zur Feststellung der Leistungspflicht müssen neben dem Schadenshergang auch die Beziehungen des Versicherten zum Schaden sowie das Bestehen eines anderweitigen Versicherungsschutzes ermittelt werden;
- 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 zu verhindern, aufzudecken und zu ermitteln, wie Betrug und Geldwäsche, 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;
- 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 rechtmasig, wenn es hierfur eine gesetzliche Grundlage gibt. Die DSGVO sieht in Art. 6 verschiedene Rechtsgrundlagen vor, die sich je nach der Art der erhobenen Daten und der Zweck deren 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 erfullen. Wenn Sie uns die relevanten personenbezogenen Daten nicht bereitstellen, sind wir unter diesen Umstanden moglicherweise nicht in der Lage, Ihnen unsere Produkte oder Dienstleistungen bereitzustellen.

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

In besonderen Fallen 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 uberwiegend dagegen sprechen. In diesem Fall erfolgt die Datenverarbeitung auf Grundlage von Art. 6 Abs. (1) lit. f) DSGVO.

7. Kategorien von Empfängern

In bestimmten Fällen geben wir einen Teil Ihrer Daten an Stellen und Personen außerhalb unseres Unternehmens weiter (siehe unten unter „Zur Erklärung“). Diese Dritten nennt das Gesetz „Empfänger von personenbezogenen Daten“. Nach Kategorien eingeordnet, geben wir Daten an folgende Gruppen von Empfängern weiter:

- Andere Unternehmen, die Teil der Konzerngesellschaft sind, sowohl in Deutschland als auch international;
- Behörden;
- Gerichte;
- Ihre Bank;
- Rechtsanwälte, die für Markel tätig werden;
- Wirtschaftsprüfer, die für Markel tätig werden;
- Externer Datenschutzbeauftragter von Markel;

- Personen, mit denen Sie im Rahmen ihres Beschäftigungsverhältnisses bei Markel in Kontakt sind;
- Dienstleister, die personenbezogene Daten verarbeiten (sog. Auftragsverarbeiter).

8. Übermittlung in ein Drittland

Die Empfänger Ihrer personenbezogenen Daten können teilweise in sogenannten Drittländern sitzen, also Ländern, deren Datenschutzniveau nicht dem der Europäischen Union entspricht. Soweit dies der Fall ist und die Europäische Kommission für diese Länder keinen Angemessenheitsbeschluss (Art. 45 DSGVO) erlassen hat, haben wir entsprechende Vorkehrungen getroffen, um ein angemessenes Datenschutzniveau für etwaige Datenübertragungen zu gewährleisten. Hierzu zählen u.a. die Standardvertragsklauseln der Europäischen Union oder verbindliche interne Datenschutzvorschriften. Wo dies nicht möglich ist, stützen wir die Datenübermittlung auf Ausnahmen des Art. 49 DSGVO, insbesondere Ihre Einwilligung oder die Erforderlichkeit der Übermittlung zur Vertragserfüllung.

EU-Standardvertragsklauseln: https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_de

9. 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. Darüber hinaus müssen Ihre personenbezogenen Daten für die Zeit aufbewahrt werden, in der Ansprüche gegen unser Unternehmen geltend gemacht werden können (gesetzliche Verjährungsfrist von 3 oder bis zu 30 Jahren). Entsprechende Nachweis- und Aufbewahrungspflichten ergeben sich aus dem Handelsgesetzbuch sowie der Abgabenordnung. Die Speicherfristen betragen danach bis zu 10 Jahre.

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.

10. Einsatz von Künstlicher Intelligenz

Um unseren Kundenservice zu verbessern und Anfragen an service@markel.de schneller beantworten zu können, nutzen wir Künstliche Intelligenz. Eingehende E-Mails werden automatisch analysiert und in vordefinierte Kategorien eingeordnet, um die Anliegen direkt an die zuständigen Mitarbeiter weiterzuleiten. Diese Klassifizierung ermöglicht es den Mitarbeitern, die Anfragen je nach Thema und Dringlichkeit zu priorisieren, wodurch eine schnellere und gezielte Bearbeitung gewährleistet wird. Die Verarbeitung erfolgt über den MS AI Builder Classifier von Microsoft.

Zusätzlich setzen wir Künstliche Intelligenz ein, um Kundenanfragen zu Versicherungsprodukten präzise beantworten zu können. Dazu gehört auch das automatische Auswerten von E-Mails, um häufige Anliegen und Muster in den Anfragen zu erkennen. Zusätzlich werden die öffentlichen Solvency Reports eingelesen, damit das KI-Modell fundierte und präzise Antworten auf Fragen zu diesem Thema liefern kann.

11. Rechte der betroffenen Person

Sie haben jederzeit das Recht unentgeltlich Auskunft (Art. 15 DSGVO) über die Verarbeitung Ihrer personenbezogenen Daten durch uns zu erhalten. Diesen Antrag können sie innerhalb eines angemessenen Zeitraums erneut stellen. Des Weiteren haben Sie das Recht, eine Kopie Ihrer Daten, die Gegenstand der Verarbeitung sind, zu erhalten.

Sofern die Daten fehlerhaft oder nicht mehr aktuell sind, haben Sie das Recht unverzüglich die Berichtigung (Art. 16 DSGVO) zu verlangen. Zudem haben Sie danach unter Berücksichtigung der Zwecke der Verarbeitung das Recht die Vervollständigung unvollständiger Daten zu Ihrer Person zu verlangen.

Sie können die Löschung (Art. 17 DSGVO) Ihrer personenbezogenen Daten verlangen, soweit nicht die Verarbeitung nach Art. 17 Abs. 3 DSGVO erforderlich ist.

Sie sind berechtigt die Einschränkung (Art. 18 DSGVO) der Verarbeitung von uns zu verlangen.

Ferner haben Sie das Recht auf Datenportabilität (Art. 20 DSGVO) sowie das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden (Art. 22 DSGVO).

Werden Ihre Daten von uns auf Grundlage von Art. 6 Abs. 1 lit. e oder f DSGVO verarbeitet, steht Ihnen ein Widerspruchsrecht gegen diese Verarbeitung unter den Voraussetzungen des Art. 21 DSGVO zu.

Außerdem haben Sie jederzeit das Recht, Ihre Einwilligung – sofern Sie eine Einwilligung in bestimmten Fällen abgegeben haben - zur Verarbeitung Ihrer Daten zu widerrufen (Art. 7 Abs. 3 DSGVO). Durch den Widerruf wird die Rechtmäßigkeit der bis zum Widerruf der Einwilligung erfolgten Verarbeitung nicht berührt.

Ihnen steht zudem ein Beschwerderecht bei einer Aufsichtsbehörde zu. Dieses können Sie beispielsweise bei einer Aufsichtsbehörde an Ihrem Wohnsitz, Ihrem Arbeitsplatz oder dem Ort des mutmaßlichen Verstoßes geltend machen. Die für Markel zuständige Datenschutzbehörde ist „das Bayerische Landesamt für Datenschutzaufsicht (BayLDA)“,
Website: https://www.lda.bayern.de/.

Wir bei Markel nehmen Ihre Betroffenenrechte ernst. Bitte zögern Sie deshalb nicht, uns unter der folgenden E-Mail-Adresse service@markel.de zu kontaktieren. Alternativ können Sie Ihre Rechte auch insbesondere per Post oder Telefon geltend machen.

12. Stand dieser Datenschutzerklärung

Diese Datenschutzerklärung wurde zuletzt im Oktober 2024 aktualisiert.