DRUCKEN UND SCANNEN NICHT NOTWENDIG ⓘ

MARKEL

Pro Cyber

CH V.1.2

Dieses Dokument beinhaltet

Fragebogen für Cyber-Versicherungen	Allgemeine Datenschutz-erklärung

FRAGEBOGEN PRO CYBER CH V.1.2

1. Angaben zum Versicherungsbetreuer

Vermittler-Name			
Maklerverband/-pool			
Vermittler-Nr.		☐ Noch keine Anbindung (www.markel.ch/fuer-makler)	
E-Mail Vermittler			

☐ **Neuantrag** ☐ **Änderungsantrag** Vertrags-Nr.

2. Angaben zum Versicherungsnehmer

Anrede	Bitte auswählen	Titel	
Vorname		Nachname	
Firmenname			
(Bitte auch Firmierung beim Firmennamen angeben)			
Webseite	www.		
E-Mail-Adresse			
Telefonnummer			
Strasse		Nr.	
PLZ		Ort	

3. Tätigkeits-, Betriebsbeschreibung

Branche gem. NOGA 2025	Bitte auswählen

CH V.1.2

4. Risikoinformation

1.	Der Tätigkeitsbereich des Antragstellers liegt in den folgenden Bereichen: – Zahlungsabwicklung, -dienstleistung, Inkassodienstleistung, – Glücksspiel oder Pornografie, – Datensammlung und -speicherung (Hauptgeschäftszweck), – Klinik, Krankenhaus, – Ratingagentur, – Direktmarketing, – Versorgungsunternehmen (bspw. Energie, Wasser, Telekommunikation).	Nein ☐
2.	Der Antragsteller speichert mehr als 10.000 personenbezogene Daten von in den USA ansässigen Personen.	Nein ☐
3.	Der Antragsteller bestätigt, dass es in den letzten 5 Jahren: – Keine Schäden durch Cyber- und Daten-Eigenschäden (bspw. Hacker-Angriff, Erpressung, Schadsoftware) oder Cyber-Drittschäden über CHF 2'500 gab, – Keine Vorfälle wie Fake-President-Angriffe oder Vertrauensschäden gab, und – Keine Umstände bekannt sind, die zu einem Schaden oder einer Inanspruchnahme führen könnten (Warnungen durch Firewalls oder Virenscanner ohne Auswirkungen sind nicht zu berücksichtigen).	Ja ☐
4.	Der Antragsteller bestätigt, dass keine Aufsichtsbehörde, staatliche Stelle oder Verwaltungsbehörde Klage gegen ihn eingereicht, Ermittlungen eingeleitet oder Auskünfte angefordert hat, was den Umgang mit sensiblen Daten angeht.	Ja ☐
5.	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 Datensicherungen (bis CHF 1'000'000 Umsatz mindestens wöchentliche, ab CHF 1'000'000 Umsatz mindestens tägliche) auf separierten Systemen oder Datenträgern (zum Beispiel NAS, externe Festplatte, separierter Server).	Ja ☐
6.	Nur zu beantworten bei einem Umsatz von **mehr** als CHF 10 Mio.: Der Antragsteller erfüllt folgende Sicherheitsvorkehrungen: – 4-Augen-Prinzip: Überweisungen über CHF 10'000 werden erst nach einer zusätzlichen Freigabe durchgeführt, – Geschützter Fernzugriff: Fernzugriffe auf Systeme mit vertraulichen Unternehmens- und personenbezogenen Daten erfolgen ausschliesslich über eine 2-Faktor-Authentifizierung (bspw. Authenticator-App) oder VPN-Tunnel, – Sichere Netzwerkinfrastruktur: Kein Zugriff auf veraltete Systeme ohne Hersteller-Sicherheitsupdates (bspw. Windows 7/XP/NT) oder Nutzung eines separaten Netzwerks für solche Systeme.	Ja ☐
7.	Nur zu beantworten bei Nutzung von **Fertigungsmaschinen**: Fertigungsmaschinen sind von externen Netzwerken und dem Unternehmensnetzwerk separiert.	Ja ☐

→ **Hinweis:** Sollten Sie die oben genannten Risikoinformationen vollständig beantworten können, kann die Anfrage auch direkt über unser Cyber-Antragsmodell zur Policierung eingereicht werden (dieses finden Sie unter www.markel.ch).

5. Unternehmen

5.1 Unternehmenskennzahlen

Bei Konzernen bitten wir um die Angabe der konsolidierten Umsätze.	Schätzung laufendes Geschäftsjahr	Letztes Geschäftsjahr
Umsatz gesamt	CHF	CHF
– davon Umsätze in der Schweiz	CHF	CHF
– davon Umsätze in der EU und dem EWR	CHF	CHF
– davon Umsätze in den USA und Kanada	CHF	CHF
– davon Umsätze online	CHF	CHF
Rohertrag	CHF	CHF

Anzahl Mitarbeiter gesamt	Anzahl IT-Mitarbeiter

5.2 Tochtergesellschaften

Tochtergesellschaften oder Niederlassungen ausserhalb der Schweiz?	Ja	Nein

Wenn JA, bitte die nachfolgenden Felder ausfüllen.

Firmenname	Land	Tätigkeit	Umsatz
			CHF
			CHF
			CHF
			CHF

6. Fragen zur organisatorischen IT-Sicherheit

5.1 Unternehmenskennzahlen

Haben Sie eine der folgenden Zertifizierungen?

ISO 9001	Ja	Nein
ISO 27001	Ja	Nein
ISIS 12	Ja	Nein
Haben Sie einen Datenschutzbeauftragten bestellt?		
Wenn ja, einen	externen oder	internen Datenschutzbeauftragten?
Haben Sie einen IT-Sicherheitsbeauftragten bestellt?		
	externen oder	internen IT-Sicherheitsbeauftragten?

CH V.1.2

6.2 Zugangssicherung

Für jeden Nutzer und Administrator ist eine benutzerindividuelle Kennung/Zugang mit Passwort vergeben.	Ja	Nein
Es erfolgt ein Account-Lockout nach maximal 5 Fehleingaben.	Ja	Nein
Es gibt eine Passwortrichtlinie deren Einhaltung (bspw. durch einen Passwortmanager) sichergestellt wird.	Ja	Nein
Für Fernzugriff auf alle Systeme in Ihrem Unternehmen ist die Multi-Faktor-Authentifizierung (MFA) implementiert.	Ja	Nein

Wie viele Personen haben Administrationsrechte?

bis zu 3 Personen	bis zu 10 Personen
bis zu 5 Personen	mehr als 10 Personen

Sind Zugriffe von Admins per Multi-Faktor-Authentifzierung (MFA) abgesichert?	Ja	Nein

6.3 IT-Notfall und Wiederanlauf Konzept

Ein IT-Notfallplan ist schriftlich fixiert und benennt Verantwortliche.	Ja	Nein
Ein Business Continuity Plan ist schriftlich fixiert und bennent Verantwortliche.	Ja	Nein
Ein Disaster Recovery Plan (Plan zur Wiederherstellung von Daten oder Systemen) ist schriftlich fixiert und bennent Verantwortliche.	Ja	Nein

6.4 Awareness

Es werden regelmässig, (mindestens jährlich,) Sensibilisierungs- und Schulungsmassnahmen zu Informationssicherheit, aktuellen Cyber-Bedrohungen und Datenschutz durchgeführt.	Ja	Nein

6.5 IT-Dienstleister

Die Datenverarbeitung (oder Teile davon) wird von Subunternehmern oder IT-Dienstleistern durchgeführt.	Ja	Nein
Die Dienstleister werden von Haftungsansprüchen freigestellt.	Ja	Nein

Bitte geben Sie an, welche IT-Dienstleister Sie in den jeweiligen Bereichen in Anspruch nehmen.

E-Mail	
Server-Betrieb	
Website	
Sonstige	

7. Risikoinformationen zur technischen Sicherheit

7.1 Schutz vor Schadsoftware

Verwenden Sie folgende technische IT-Sicherheitssysteme?

Hardware-Firewall	mit automatischen Updates	Ja	Nein
Hersteller:			
Software-Firewall	mit automatischen Updates	Ja	Nein
	Standard-Firewall über Betriebssystem		
	Lizenzierte Firewall von Drittanbietern		
Hersteller:			
Viren-Scanner	mit automatischen Updates	Ja	Nein
	Standard-Virenscanner über Betriebssystem		
	Lizenzierter Viren-Scanner von Drittanbietern		
Hersteller:			

Sofern die oben genannten IT-Sicherheitssysteme manuell geupdatet werden, in welchem Turnus werden die Updates vorgenommen?

täglich	monatlich
wöchentlich	sonstiges:

7.2 Datensicherung

Erstellen Sie für Ihre Daten und Programme Back-Ups?

täglich	monatlich
wöchentlich	sonstiges:

Speichermedium

weiterer Server	Cloud:
Festplatte	sonstiges:

In Ihrem Unternehmen wird mindestens einmal jährlich ein Wiederherstellungstest für alle Datensicherungen durchgeführt.	Ja	Nein
Die Backups des Hauptdatenspeichers werden räumlich getrennt aufbewahrt und durch Administratorrechte abgesichert	Ja	Nein

7.3 IT-Systeme und Netzwerk

Werden „End-of-Life"-Systeme genutzt (Systeme, für die der Hersteller keine Sicherheitsupdates oder Support mehr bereitstellt)?	Ja	Nein

Falls ja:

a) Werden diese in einer isolierten Netzwerkumgebung betrieben?	Ja	Nein
b) Besteht eine direkte Verbindung zum externen Netzwerk (Internet)?	Ja	Nein
c) Gibt es einen Migrationsplan?	Ja	Nein

Wird eine „Endpoint-Protection-Lösung"(EDR), welche automatisch aktualisiert wird, eingesetzt?	Ja	Nein
Wird ein 24/7 Security Operations Center (SOC) eingesetzt, das sicherheitsrelevante Ereignisse kontinuierlich überwacht und bei Bedarf Massnahmen zur Gefahrenisolierung ergreifen kann?	Ja	Nein
Findet eine automatisierte Überwachung, Protokollierung und Überprüfung von Protokolldateien (SIEM) statt?	Ja	Nein

Ist im Rahmen des Patch Managements folgendes sichergestellt?

Sicherheitspatches werden innerhalb von vier Wochen installiert.	Ja	Nein
Kritische Sicherheitspatches und Hinweise für IT-Bedrohungslagen mit einem CVSS-Score (Common Vulnerability Scoring System) von 8.0 oder höher werden unverzüglich behandelt.	Ja	Nein

Wie schnell würde der Umsatz Ihres Unternehmens durch einen Cyber-Vorfall oder einen Ausfall / eine Störung des IT-Systems beeinträchtigt?

< 8 Stunden	< 3 Tage
< 12 Stunden	< 1 Woche
< 24 Stunden	sonstiges:

Wie schnell können Sie Ihr IT-System nach einem Cyber-Vorfall oder einem Ausfall / einer Störung wieder in Notbetrieb nehmen (Wiederanlaufzeit)?

< 8 Stunden	< 3 Tage
< 12 Stunden	< 1 Woche
< 24 Stunden	sonstiges:

8. Operative und Produktions-Technologie

Hinweis: sofern Sie keine ICS Systeme (Industrial Control Systems) oder andere Produktionsanlagen haben können Sie diesen Punkt überspringen.

Die automatisierten Kontrollsysteme befinden sich auf einem separierten Netzwerk.	Ja	Nein
Fernzugriffe sind mittels VPN Verbindung abgesichert.	Ja	Nein
Fernzugriffe sind mittels MFA abgesichert	Ja	Nein
Fernzugriffe werden durchgehend protokolliert.	Ja	Nein
Die Produktion kann bei einem Ausfall der IT-Systeme manuell fortgesetzt werden.	Ja	Nein

9. Risikoinformationen zu Zahlungsmethoden

Bieten Sie Ihren Kunden Onlinezahlungsmethoden an?	Ja	Nein
Wenn JA, dann beantworten Sie bitte die folgenden Frage:		
Speichern und verarbeiten sie hierbei Bank- oder Kreditkartendaten selbst?	Ja	Nein
Wenn JA, dann beantworten Sie bitte die folgenden Frage:		
Anzahl der Bank- oder Kreditkartendaten:		
Werden Überweisungen über 10 ‘000 CHF im 4-Augen-Prinzip geprüft?	Ja	Nein

10. Risikoinformationen zu personenbezogenen Daten

Speichern und verarbeiten sie personenbezogene Daten?	Ja	Nein
Wenn ja, von wie vielen Personen liegen personenbezogene Daten vor?	Anzahl:	
Von wie vielen Personen liegen Gesundheitsdaten und / oder Finanzdaten vor?	Anzahl:	

11. Versicherungssumme

Versicherungssumme für alle Bausteine der Cyber-Versicherung pauschal für alle Bausteine je Versicherungsfall und - jahr:

CHF 100‘000	CHF 2‘000‘000
CHF 250‘000	CHF 3‘000‘000
CHF 500‘000	CHF 5‘000‘000
CHF 1‘000‘000	CHF

12. Abwahlmöglichkeit der Bausteine ohne Nachlass Angaben

Baustein A.2	Abwahl Cyber-Betriebsunterbrechung
Baustein A.3	Abwahl Cyber-Erpressung
Baustein A.4	Abwahl Cyber-Zahlungsmittel
Baustein A.5	Abwahl Cyber-Vertrauensschaden
Baustein A.6	Abwahl Cyber-Haftpflicht
Baustein A.7	Abwahl Prävention Premium analog zu den oberen Bausteine

13. Selbstbeteiligung

je Versicherungsfall				
CHF 500	CHF 1‘000	CHF 2‘500	CHF 5‘000	CHF

14. Vorversicherung

Versicherer			
Versicherungssumme		Jahresnettoprämie	CHF
Dauer der Nachhaftung			
Kündigung der Vorversicherung durch den	Versicherer		Versicherungsnehmer
Gründe für die Kündigung			

15. Vorschäden

Bei dem Versicherungsnehmer oder anderen mitversicherten Personen sind in den vergangenen 5 Jahre Schäden im Zusammenhang mit den versicherten Bausteinen A.1 bis A.6 eingetreten, insbesondere Hacker-Angriffe/-Eingriffe und Infektionen mit Schadsoftware und/oder es sind Umstände bekannt, die zu einem Schaden führen können.*	Nein

→ Sollte die oben genannte Vorschadensinformation **nicht** mit **NEIN** beantwortet werden können, nennen Sie uns bitte Details auf einem separaten Beiblatt.

* A.1 Cyber- und Daten-Eigenschäden | A.2 Cyber-Betriebsunterbrechung | A.3 Cyber-Erpressung | A.4 Cyber-Zahlungsmittel | A.5 Cyber-Vertrauensschaden | A.6 Cyber-Haftpflicht

16. Schlusserklärung

Diese ausgefüllte Erklärung sowie eventuelle 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 Regelung des Versicherungsvertragsgesetzes (VVG). Mit Ihrer Unterschrift bestätigen Sie, dass vorstehende Angaben vollständig und richtig sind.

Mit Ihrer Unterschrift bestätigen Sie ferner, dass Sie unsere Allgemeine Datenschutzerklärung erhalten und deren Inhalt – insbesondere Ihre Rechte als Betroffener – zur Kenntnis genommen haben. Im Rahmen der Durchführung des Versicherungsvertrages sind wir auf die Verarbeitung von allgemeinen und personenbezogenen Daten angewiesen, welche wir unter Beachtung der massgeblichen datenschutzrechtlichen Vorschriften und Einhaltung der gesetzlich vorgeschriebenen Standards verarbeiten, speichern und löschen.

→ ☐ **Hiermit bestätige ich die Schlusserklärung.**

Durch wen erfolgt die Bestätigung?

☐ Versicherungsnehmer

☐ Versicherungsbroker/-betreuer

Name des Bestätigenden (keine Unterschrift notwendig)	Datum

Antrag prüfen und Versand vorbereiten

Bitte drucken Sie diesen Antrag nicht aus, sondern senden Sie uns diesen am Computer ausgefüllt zurück.

CH V.1.2

ALLGEMEINE DATENSCHUTZERKLÄRUNG

Dies ist unsere allgemeine Datenschutzerklärung, in der wir erläutern, wie wir Personendaten verwenden, die wir über Personen erfassen. Für die Nutzung unserer Webseite haben wir eine gesonderte Datenschutzerklärung, die Sie beim Besuch unserer Webseite unter https://markel.ch/datenschutzerklaerung aufrufen können.

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

1. Begriffsbestimmungen

Unsere Datenschutzerklärung beruht auf den Begrifflichkeiten, die im Schweizerischen Bundesgesetz über den Datenschutz (DSG) 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 Personendaten

Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.

1.2 Betroffene Person

Betroffene Person ist jede natürliche Person, über die Personendaten bearbeitet werden.

1.3 Bearbeitungen

Bearbeitung ist jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.

1.4 Profiling

Profiling ist jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Personendaten 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.

1.5 Verantwortlicher oder für die Bearbeitung Verantwortlicher

Verantwortlicher ist eine private Person oder ein Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung von Personendaten entscheidet.

1.6 Auftragsbearbeiter

Auftragsbearbeiter ist eine private Person oder ein Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet.

2. Verantwortlicher

Markel Insurance SE, München
Schweizer Zweigniederlassung Zürich
Limmatquai 4
CH-8001 Zürich

3. Name und Anschrift des Datenschutzberaters

Der Datenschutzberater des für die Bearbeitung Verantwortlichen ist:

Dr. Reto Fanger (Advokatur Fanger)
Sempacherstrasse 5,
CH-6002 Luzern
reto.fanger@advokatur-fanger.ch

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

4. Datenbearbeitung

Die Personendaten, die wir über Sie und andere Personen bearbeiten, 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 Personendaten bearbeiten.

Es werden verschiedene Arten von Personendaten 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 Personendaten in verschiedener Weise, wenn Sie zum Beispiel ein Versicherungsbroker 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 Personendaten, die wir speichern und bearbeiten, abhängig vom Verhältnis, in dem Sie mit uns stehen, unter anderem folgende Arten von Personendaten:

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. Bei einer Pflichtversicherung 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, Führerausweisnummer 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 Besonders schützenswerte Personendaten

Informationen über Gesundheitsdaten oder sonstige sensible Informationen wie zum Beispiel religiöse Ansichten, ethnische Zugehörigkeit, politische Ansichten oder sexuelle Orientierung beschaffen und verwenden wir grundsätzlich nicht. Sollte dies ausnahmsweise dennoch einmal der Fall sein, holen wir uns von der betroffenen Person 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 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 Personendaten 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 verwenden (unter anderem werden wir auch Ihre Einwilligung einholen, wenn dies erforderlich ist).

5. Zweck der Datenverarbeitung

Wir verwenden Personendaten, um unsere Geschäftstätigkeiten auszuführen.

Die Zwecke, für die wir Ihre Personendaten oder die von anderen Personen verwenden, 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. Personendaten werden für andere Zwecke verwandt, wenn Sie ein Versicherungsnehmer sind, als wenn Sie ein Versicherter oder ein Anspruchsteller aus einer Versicherungspolice, ein kommerzieller Versicherungsbroker oder ein bestellter Vertreter, ein Zeuge oder eine sonstige Person, mit der wir in Beziehung stehen, sind.

Die wesentlichen Zwecke, für die wir Personendaten nutzen, sind:

- zur Prüfung eines aufgetretenen Schadenfalls. Zur Feststellung der Leistungspflicht müssen neben dem Schadenshergang, 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 Personendaten wir beschaffen, 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 Personendaten verwenden und bekanntgeben, wenn dies hilfreich ist, um Ihnen ein vollständiges Bild darüber wiederzugeben, wie wir Personendaten beschaffen und verwenden. 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 Personendaten 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 Datenbearbeitung

Die Bearbeitung von Personendaten ist nur rechtmässig, wenn es hierfür eine gesetzliche Grundlage gibt. Das schweizerische DSG 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. 31 Abs. (2) lit. a) DSG Personendaten von Ihnen einholen und bearbeiten, um den Abschluss eines Versicherungsvertrags mit Ihnen vorzubereiten oder einen abgeschlossenen Versicherungsvertrag mit Ihnen abzuwickeln und / oder zu erfüllen. Wenn Sie uns die relevanten Personendaten nicht bereitstellen, sind wir unter diesen Umständen möglicherweise nicht in der Lage, Ihnen unsere Produkte oder Dienstleistungen bereitzustellen.

Teilweise müssen wir Personendaten bei Ihnen einholen und verarbeiten, um geltenden gesetzlichen Anforderungen zu entsprechen. Rechtsgrundlage hierfür bildet dann Art. 31 Abs. (1) Teilsatz 3 DSG.

In besonderen Fällen ist eine Bearbeitung erhobener Daten auch dazu notwendig, unsere berechtigten Interessen oder die eines Dritten zu wahren, sofern nicht die Interessen der betroffenen Person überwiegend dagegen sprechen. In diesem Fall erfolgt die Datenbearbeitung auf Grundlage von Art. 31 Abs. (1) Teilsatz 2 DSG.

7. Routinemässige Löschung und Sperrung von Personendaten

Der für die Bearbeitung Verantwortliche bearbeitet und speichert Personendaten der betroffenen Person nur für den Zeitraum, der zur Erreichung des Speicherzwecks erforderlich ist, oder sofern dies durch den Gesetzgeber in Gesetzen oder Vorschriften, welchen der für die Bearbeitung Verantwortliche unterliegt, vorgesehen wurde. Darüber hinaus müssen Ihre Personendaten für die Zeit aufbewahrt werden, in der Ansprüche gegen unser Unternehmen geltend gemacht werden können (gesetzliche Verjährungsfrist). Entsprechende Nachweis- und Aufbewahrungspflichten ergeben sich aus den gesetzlichen Vorgaben. Die Speicherfristen betragen danach bis zu 10 Jahre.

Entfällt der Speicherungszweck oder läuft eine vom Gesetzgeber vorgeschriebene Speicherfrist aus, werden die Personendaten routinemässig und entsprechend den gesetzlichen Vorschriften gesperrt oder gelöscht.

8. Rechte der betroffenen Person

Sie haben die Möglichkeit, jederzeit von Ihren „Betroffenenrechten“ gemäss Art. 15 DSG Gebrauch zu machen:

- Recht auf Auskunft gemäss Art. 25 DSG.
- Recht auf Berichtigung gemäss Art. 32 Abs. (1) DSG.
- Recht auf Löschung gemäss Art. 32 Abs. (2) lit. a) DSG.
- Recht auf Verbot der Bearbeitung gemäss Art. 32 Abs. (2) lit. a) DSG.
- Recht auf Datenübertragbarkeit gemäss Art. 28 Abs. (1) DSG.

Sofern Sie von Ihren Rechten Gebrauch machen möchten, richten Sie Ihr Anliegen bitte per E-Mail an service@markel.ch oder per Briefpost an die in Punkt 2 genannte Anschrift. Daneben haben Sie ein Recht auf Beschwerde bei der Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (http://www.edoeb.admin.ch).

IHR SPEZIALVERSICHERER FÜR
GEWERBLICHE HAFTPFLICHT

Markel Insurance SE, München
Schweizer Zweigniederlassung Zürich
Limmatquai 4
CH-8001 Zürich

+41 43 883 223 7

service@markel.ch
www.markel.ch