HINWEIS FÜR VERMITTLER

Pro Cyber v2

Dieses Dokument beinhaltet

Fragebogen für Cyber-Versicherungen

Allgemeine Datenschutz-erklärung

Stand Version 2

FRAGEBOGEN PRO CYBER V2

1. Angaben zum Versicherungsbetreuer

Vermittler-Name	
Maklerverband/-pool	
Vermittler-Nr.	☐ Noch keine Anbindung (www.markel.de/anbindung)
E-Mail Vermittler	

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

2. Angaben zum Versicherungsnehmer

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

3. Tätigkeits-, Betriebsbeschreibung

Branche	Bitte auswählen

Stand Version 2

4. Risikoinformation

1. Der Tätigkeitsbereich des Antragstellers liegt in den folgenden Bereichen: – Zahlungsabwicklung, -dienstleistung, Inkassodienstleistung – Glücksspiel, Pornografie, Datensammlung und -speicherung (Hauptgeschäftszweck) – Klinik, Krankenhaus – Ratingagentur, Direktmarketing – Versorgungsunternehmen (z. B. Energie, Wasser, Telekommunikation)	Nein ☐
2. Der Antragssteller speichert personenbezogenene Daten von in den USA ansässigen Personen.	Nein ☐
3. Hat der Antragsteller in den letzten 5 Jahren Schäden durch Cyber- und Daten-Eigenschäden (z. B. Hacker-Angriffe, Erpressung, Schadsoftware) oder Cyber-Drittschäden über 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 ☐
4. 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 ☐
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 (bis 1.000.000 € Umsatz mindestens wöchentliche, ab 1.000.000 € Umsatz mindestens tägliche) Datensicherungen auf separierten Systemen oder Datenträgern (zum Beispiel NAS, externe Festplatte, separierter Server).	Ja ☐
6. Bei einem Umsatz größer als 10 Millionen € ist nachfolgende Risikoinformation zusätzlich zu beantworten. Der Antragsteller nutzt darüber hinaus folgende Sicherheitsvorkehrungen: – 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 Netzwerks 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. – Einsatz von Fertigungsmaschinen: Die Fertigungsmaschinen sind von externen Netzwerken und dem Unternehmensnetzwerk separiert.	Ja ☐

→ Sollten Sie die oben genannten Risikoinformationen vollständig beantworten, können Sie gerne unser Antragsmodell verwenden (dieses finden Sie unter www.markel.de).

5. Unternehmen

5.1 Unternehmenskennzahlen

Bei Konzernen bitten wir um die Angabe der konsolidierten Umsätze.	Schätzung laufendes Geschäftsjahr	Letztes Geschäftsjahr
Umsatz gesamt	€	€
– davon Umsätze EU, EWR, Schweiz	€	€
– davon Umsätze in den USA/Kanada	€	€
– davon Umsätze im Rest der Welt	€	€
– davon Umsätze online	€	€
Rohertrag	€	€

Anzahl Mitarbeiter gesamt	Anzahl IT-Mitarbeiter

5.2 Tochtergesellschaften

Gibt es Tochtergesellschaften oder Niederlassungen **außerhalb** des EWR?			Ja ☐ Nein ☐
Wenn **JA**, bitte die nachfolgenden Felder ausfüllen.			
Firmenname	Land	Tätigkeit	Umsatz
			€
			€
			€
			€

6. Fragen zur organisatorischen IT-Sicherheit

6.1 IT-Sicherheitsmanagement

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? Wenn ja, einen externen oder internen IT-Sicherheitsbeauftragten?	

6.2 Zugangssicherung

Für jeden Nutzer und Administrator ist eine benutzerindividuelle Kennung/Zugang mit Passwort vergeben.	Ja ☐ Nein ☐
Wir haben Mindestanforderungen an die Passwortqualität sämtlicher Mitarbeiter und Systeme. Diese werden technisch erzwungen	Ja ☐ Nein ☐
Für Fernzugriff auf alle Systeme in Ihrem Unternehmen ist die Multi-Faktor-Authentifizierung (MFA) implementiert.	Ja ☐ Nein ☐

Wie viele Personen haben Administrationsrechte? Werden Zugriffsrechte nach Personen beschränkt?

☐ 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

Wird die Datenverarbeitung (oder Teile davon) 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 Standard-Firewall über Betriebssystem Lizenzierte Firewall von Drittanbietern	Ja ☐ Nein ☐
Hersteller:		
Viren-Scanner	mit automatischen Updates Standard-Virenscanner über Betriebssystem Lizenzierter Viren-Scanner von Drittanbietern	Ja ☐ Nein ☐
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) Sind 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 Fragen:	
Speichern und verarbeiten sie hierbei Bank- oder Kreditkatendaten selbst?	Ja ☐ Nein ☐
Wenn Sie diese selbst verarbeiten: Anzahl der Bank- oder Kreditkartendaten:	
Werden Überweisungen über 10.000 € 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 Finanzdaten vor ? Anzahl:	

11. Versicherungssumme

Versicherungssumme für alle Bausteine der Cyber-Versicherung pauschal für alle Bausteine je Versicherungsfall und - jahr:	
100.000 €	2.000.000 €
250.000 €	3.000.000 €
500.000 €	5.000.000 €
1.000.000 €	€

Stand Version 2

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				
500 €	1.000 €	2.500 €	5.000 €	€

14. Vorversicherung

Versicherer			
Versicherungssumme	€	Jahresnettoprämie	€
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 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 ☐ Versicherungsmakler/-betreuer

Name des Bestätigenden (keine Unterschrift notwendig)	Datum

Fragebogen versenden

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

Stand Version 2

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.

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 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 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 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.

In bestimmten Fällen erfolgt die Datenverarbeitung aufgrund Ihrer Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO bzw. Art. 9 Abs. 2 lit. a 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.