HISCOX

Bitte per Telefax oder E-Mail an
Carl Rieck GmbH
Fax-Nr.: +49 (0)6074 69665 11
E-Mail: hiscox@carlrieck.de

CARL RIECK ASSECURADEUR

Fragebogen CyberClear

Mit diesem Fragebogen möchten wir Sie und Ihr Unternehmen gerne kennenlernen. Aufgrund der von Ihnen gemachten Angaben besteht für keine Partei die Verpflichtung zum Abschluss eines Versicherungsvertrages.

Bitte beantworten Sie die folgenden Fragen vollständig und verwenden Sie falls notwendig ein Beiblatt.

I. GENERELLE INFORMATIONEN

Vermittlername | Vermittlernummer

1. Unternehmensangaben

Name | Homepage

Straße, Nr. | Tätigkeitsbeschreibung (Branche und Geschäftstätigkeit)

PLZ, Ort, Land

2. Unternehmenskennzahlen

Konsolidierte Kennzahlen für alle mitzuversichernden Gesellschaften aus dem letzten Geschäftsjahr

	Gesamt	davon EWR	davon USA/Kanada	davon restliche Länder
Umsatz in €				
davon Onlineumsatz in €				
Rohertrag in €				
Anzahl Mitarbeiter				
Anzahl Kunden				

Gesamtumsatz aktuelles Geschäftsjahr in € _____

3. Mitzuversichernde Gesellschaften

Tochtergesellschaften außerhalb des Europäischen Wirtschaftsraumes (EWR) und/oder mitzuversichernde Gesellschaften im In- und Ausland inkl. Tätigkeit und Umsatz (ggf. auf separatem Blatt).

Name	Anschrift	Umsatz in €	Tätigkeit (falls abweichend)

Bitte fügen Sie dem Fragebogen ggf. ein aktuelles Organigramm der Unternehmensstruktur bei.

Hinweis: Die nachfolgenden Fragen bitte für die Gesamtheit der zu versichernden Unternehmen beantworten.
Bei Abweichungen bitten wir um weitere Informationen auf einem separaten Blatt.

4. Versicherungsumfang

Versicherungs-summe	☐ € 500.000	☐ € 1.000.000	☐ € 3.000.000	☐ € 5.000.000	☐ € _____
Selbstbehalt	☐ € 5.000	☐ € 10.000	☐ € 25.000	☐ € 50.000	☐ € _____

Bitte per Telefax oder E-Mail an
Carl Rieck GmbH
Fax-Nr.: +49 (0)6074 69665 11
E-Mail: hiscox@carlrieck.de

Ist eine Absicherung von Cyber-Diebstahl und/oder Cloud-Ausfall und/oder Vertragsstrafen wegen verzögerter Leistungserbringung gewünscht? **Wenn keine Absicherung gewünscht, bitte mit 5. Zusatzfragen fortfahren.**

Diese Frage ist nur zu beantworten, wenn die Erweiterung Cyber-Diebstahl gewünscht wird.

1. Haben Sie bei Ihren Telefonanlagen und Anrufbeantwortern die Passwörter & PINs von der Werkseinstellung geändert? ☐ Ja ☐ Nein
2. Haben Sie ein verpflichtendes Vier-Augen-Prinzip ab einer Überweisungshöhe von € 25.000 implementiert? ☐ Ja ☐ Nein

Diese Fragen sind nur zu beantworten, wenn die Erweiterung Betriebsunterbrechung bei Cloud-Ausfall gewünscht wird.

1. Welche kritischen Geschäftsprozesse haben Sie in die Cloud ausgelagert? _____
2. Welche Verfügbarkeit haben Sie mit ihrem Cloud-Anbieter vereinbart? Zugesicherte Betriebszeit _____ %

☐ Tier Level 1 ☐ Tier Level 2 ☐ Tier Level 3 ☐ Tier Level 4

☐ TUViT Level 1 ☐ TUViT Level 2 ☐ TUViT Level 3 ☐ TUViT Level 4

3. Welche zusätzlichen Zertifizierungen werden von Ihrem Cloud-Anbieter vorgehalten?

☐ ISO27001 ☐ IT Grundschutz ☐ BSI C5 ☐ Andere _____

Wünschen Sie die Erweiterung um Vertragsstrafen wegen verzögerter Leistungserbringung? ☐ **Ja** ☐ **Nein**
Falls ja, fügen Sie die vertragliche Vereinbarung bitte dem Fragebogen an.

5. Zusatzfragen

Können Ihre Kunden bei Ihnen mit Kreditkarte zahlen? ☐ Ja ☐ Nein
Falls ja, dann beantworten Sie bitte die Fragen zur Kreditkartenzahlung auf Seite 1 des Zusatzfragebogens.

Generieren Sie Onlineumsätze über Ihre Website? ☐ Ja ☐ Nein
Falls ja, dann beantworten Sie bitte die Fragen zum Online Shop auf Seite 2 des Zusatzfragebogens.

Betreiben Sie Industrie-Steuerungsanlagen mithilfe automatisierter Kontrollsysteme (ICS/SCADA) z.B. Produktion oder Logistik? ☐ Ja ☐ Nein
Falls ja, dann beantworten Sie bitte die Fragen zu Industrie-Steuerungsanlagen auf Seite 3 des Zusatzfragebogens.

II. DATEN

1. Datenschutz

1. Bitte kreuzen Sie die Spanne der sensiblen personenbezogenen Datensätze an, die Ihr Unternehmen sammelt, verarbeitet und speichert: **(Zutreffendes bitte ankreuzen)**

Sensible personenbezogene Daten sind 1. Sozialversicherungs-, Führerschein- und Ausweisdaten 2. Steuer und Finanzdaten, wie Bank- oder Kreditkartenkonten 3. Informationen zu Strafverfahren und Ordnungswidrigkeiten 4. Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

☐ 0 – 20.000 ☐ 20.001 – 100.000 ☐ 100.001 – 250.000

☐ 250.001 – 500.000 ☐ 500.001 – 1.000.000 ☐ > 1.000.000

Bei Datenmengen größer 1.000.000 bitten wir um eine genauere Aufschlüsselung (in 1. bis 4.) und die konkrete Anzahl.

2. Führen Sie ein Verfahrensverzeichnis (BDSG) bzw. Verzeichnis von Verarbeitungstätigkeiten (EU-DSGV) bezüglich des Umgangs mit personenbezogenen Daten? ☐ Ja ☐ Nein
3. Sind jährliche Reports des Datenschutzbeauftragten vorhanden? ☐ Ja ☐ Nein
4. Gibt es in Ihrem Unternehmen eine Prüfung ob datenschutzrechtliche Vorgaben eingehalten werden?

☐ Nicht regelmäßig ☐ Nur bei kritischen Änderungen ☐ Mindestens einmal jährlich

Bitte per Telefax oder E-Mail an
Carl Rieck GmbH
Fax-Nr.: +49 (0)6074 69665 11
E-Mail: hiscox@carlrieck.de

2. Datenverarbeitung

1. Sind Sie im Rahmen der Auftragsdatenverarbeitung für Dritte tätig? ☐ Ja ☐ Nein

2. Nutzen Sie Dienstleister zur Auftragsdatenverarbeitung? ☐ Ja ☐ Nein

Nr.	Name des Dienstleisters	E-Mail	Hosting	Abrechnung	Sonstige	Sofern Haftungsfreistellungen vereinbart, in welcher Form?
1.		☐	☐	☐		
2.		☐	☐	☐		
3.		☐	☐	☐		

Wenn genutzt bitte in der Tabelle aufführen, wenn nicht bitte mit Teil III. fortfahren (ggf. auf separatem Blatt).

3. Halten sich Ihre Dienstleister mindestens an das Datenschutzniveau aus Ihrem Unternehmen und überprüfen Sie dies regelmäßig durch Auditierungen?

☐ Nein bzw. unbekannt ☐ Ja, wir lassen uns dies regelmäßig durch eine Selbstauskunft bestätigen ☐ Ja, wir überprüfen dies regelmäßig durch die Prüfung eines Auditors ☐ Ja, unser Dienstleister ist zertifiziert. Benennung Zertifikat: _____

4. Regeln Sie in Ihren Dienstleistungsverträgen die Verfügbarkeit, Updates und das Beheben von Sicherheitslücken? ☐ Ja ☐ Nein

III. INFORMATIONSSICHERHEITS-MANAGEMENT

1. ISMS Zertifizierung

1. Ist in Ihrem Unternehmen ein Informationssicherheits-Management-System (ISMS) etabliert? ☐ Ja ☐ Nein
Wenn ja, von wem wird das ISMS überprüft und angepasst?

☐ Eigene IT-Abteilung ☐ Interne(r) Informationssicherheitsbeauftragte(r) ☐ Interne Revision

☐ Externer Wirtschaftsprüfer ☐ Sonstige _____

2. Sind Sie nach einem der folgenden Standards oder Normen zertifiziert? ☐ Ja ☐ Nein

Wenn vorhanden, bitte angeben und mit Teil IV. fortfahren.

☐ VdS 3473 ☐ ISO27001 ☐ IT-Grundschutz ☐ Cloud C5 Anforderung Katalog - Testat nach BSI C5

Bis wann ist diese Zertifizierung gültig? _____ Ist eine Verlängerung beabsichtigt? ☐ Ja ☐ Nein

2. Technische Sicherheitsmaßnahmen

1. Verfügen alle informationsverarbeitenden Systeme über einen Virenschutz mit aktuellen Virensignaturen? ☐ Ja ☐ Nein

2. Betreiben Sie Firewallstrukturen an allen Netzübergängen zu externen Netzen? ☐ Ja ☐ Nein

3. Wer (Position) ist in Ihrem Unternehmen für die IT-Sicherheit verantwortlich?

☐ GeschäftsführerIn ☐ IT-Sicherheitsbeauftragte(r) / CISO ☐ IT-LeiterIn ☐ Sonstige _____

4. Haben Sie eine Richtlinie implementiert, die durchgehend das automatische oder zeitnahe Einspielen von Sicherheitsupdates regelt (Patch-Management-Prozess)? ☐ Ja ☐ Nein

- Sind hiervon auch Plug-Ins (Webbrowser und Frameworks) erfasst? ☐ Ja ☐ Nein

5. Sind die IT-Systeme die mit Außen kommunizieren in einem separaten Segment gebündelt? (Demilitarisierte Zone (DMZ)) ☐ Ja ☐ Nein

- Ist das interne Netz noch weiter segmentiert (Client, Server, Multifunktionsgeräte)? ☐ Ja ☐ Nein
- Erfolgt zwischen den Segmenten eine Filterung der Kommunikation? ☐ Ja ☐ Nein

Bitte per Telefax oder E-Mail an
Carl Rieck GmbH
Fax-Nr.: +49 (0)6074 69665 11
E-Mail: hiscox@carlrieck.de

6. Sie haben eine IT-Sicherheitsrichtlinie umgesetzt, in der die folgenden Elemente geregelt werden: **(Zutreffendes bitte ankreuzen)**

- ☐ Wir haben keine schriftliche IT-Sicherheitsrichtlinie
- ☐ Benutzerindividuelle Zugänge mit erzwungenen individuellen Passwörtern
- ☐ Alle Standardnutzer und Standardpasswörter werden durch starke individuelle Daten ersetzt
- ☐ Definierte Mindestanforderungen an die Passwortstärke
- ☐ Zugriffsbeschränkungen, sodass jeder Mitarbeiter nur auf die Ressourcen (Daten und Programme) Zugriff hat, die für das jeweilige Aufgabenspektrum benötigt werden
- ☐ Prozess zur regelmäßigen Überprüfung der Zugriffsrechte (z.B. bei Beförderung oder Kündigung)
- ☐ Administrative Zugänge werden ausschließlich zur Erledigung administrativer Tätigkeiten genutzt. Für die alltägliche Nutzung (insbesondere Surfen im Internet) wird ein Benutzer-Konto ohne Admin-Rechte verwendet
- ☐ Dauer der Speicherung von Protokollierungsdaten
- ☐ Authentifizierungsverfahren wie Mehr-Faktor-Authentifizierung, Zertifikate, Hard-Token, Einmalpasswörter
- ☐ Sichere Vernichtung von sensiblen Daten
- ☐ Regelung oder Verbot der privaten Nutzung der dienstlichen IT Infrastruktur
- ☐ Vorhalten eines aktuellen Netzplans (Strukturplan des IT-Systems)

7. Welche Maßnahmen haben Sie zur Erkennung von Angriffen und Sicherheitsvorfällen implementiert? **(Zutreffendes bitte ankreuzen)**

- ☐ Wir haben keine entsprechenden Maßnahmen implementiert
- ☐ Automatische Auswertung von Protokolldaten
- ☐ Angriffserkennungssystem (Intrusion-Detection und -Prevention)
- ☐ Schutzmaßnahmen gegen unerwünschten Datenabfluss (Data Loss Prevention)
- ☐ System zum Umgang mit sicherheitsrelevanten Ereignissen (Security Information und Event Management (SIEM))
- Ist sichergestellt, dass bei Feststellung unmittelbar eine Bewertung und Lösung umgesetzt wird? ☐ Ja ☐ Nein

8. Wurde in der Vergangenheit ein Penetrationstest durchgeführt? ☐ Ja ☐ Nein
Wenn ja, wann zuletzt? _____

9. Sie haben in Ihrem Unternehmen folgende Schutzmaßnahmen bei Fernwartungszugängen und Fernzugriffen umgesetzt: **(Zutreffendes bitte ankreuzen)**

- ☐ Fernwartungszugänge und Fernzugriffe sind nicht möglich
- ☐ Dokumentation der eingerichteten Fernwartungszugänge und Fernzugriffe
- ☐ Geeignete VPN-Verschlüsselung (Virtual Private Networks)
- ☐ Personenbezogene Zugänge
- ☐ Zwei-Faktor-Authentifizierung
- ☐ Protokollierung des Verbindungsaufbaus und Archivierung der Daten
- ☐ Protokollierung aller Tätigkeiten beim Zugriff durch Externe
- ☐ Beobachtung externer Wartungszugriffe durch eigene Mitarbeiter
- ☐ Interne individuelle Freischaltung nur für Dauer und Zweck der Fernwartung

10. Sie haben in Ihrem Unternehmen eine Mobilgeräteverwaltung (Mobile-Device-Management (MDM)) implementiert, das die folgenden Schutzmaßnahmen umsetzt: **(Zutreffendes bitte ankreuzen)**

- ☐ Wir haben kein MDM umgesetzt
- ☐ Fernlöschung der Geräte
- ☐ Sichere VPN Verbindung (beschränkt, protokolliert, autorisiert)
- ☐ Verschlüsselung (Full-disk-encryption)
- ☐ Abgetrennte Container für dienstliche Daten auf mobilen Geräten
- ☐ Es gibt eine Bring-Your-Own-Device-Policy (BYOD) - Regelung zur dienstlichen Nutzung privater Geräte

3. Datensicherung

1. Führen Sie mindestens täglich eine automatische Sicherung durch? ☐ Ja ☐ Nein
Wenn nein, dann _____

2. Wird die Datensicherung von der Betriebsumgebung getrennt gespeichert? ☐ Ja ☐ Nein

Bitte per Telefax oder E-Mail an
Carl Rieck GmbH
Fax-Nr.: +49 (0)6074 69665 11
E-Mail: hiscox@carlrieck.de

3. Ist die Datensicherung durch Verschlüsselung und beschränkte Zugriffsrechte vor Manipulation geschützt? ☐ Ja ☐ Nein

4. In welchem Turnus wird die Wiederherstellung dieser Daten getestet?

☐ Gar nicht ☐ Unregelmäßig ☐ Jährlich ☐ Quartalsweise ☐ Monatlich

IV. NOTFALLMANAGEMENT

1. Haben Sie kritische IT-Systeme und Anwendungen für Ihr Unternehmen definiert und diese redundant aufgestellt? ☐ Ja ☐ Nein

2. Haben Sie die für Ihr Unternehmen kritischen bzw. sensiblen Daten definiert? ☐ Ja ☐ Nein

3. Sie betreiben Business Continuity Management (BCM) inkl. IT-Notfallplan und Wiederanlauf-Konzept der betriebsnotwenigen Systeme in Ihrem Unternehmen und setzen dabei Folgendes um: **(Zutreffendes bitte ankreuzen)**

☐ Wir haben kein BCM umgesetzt
☐ Schriftlich fixiertes BCM
☐ Benannte verantwortliche Person(en) für BCM
☐ Regelmäßige inhaltliche Überprüfung
☐ Regelmäßige praktische Tests
☐ Ausgerichtet an einer Norm (BSI 100-4 oder ISO22301)
☐ ISO22301 zertifiziert

V. VORSCHÄDEN

1. Hat eine Aufsichtsbehörde, staatliche Stelle oder Verwaltungsbehörde Klage gegen Sie oder eine mitversicherte Person eingereicht, Ermittlungen eingeleitet oder Auskünfte angefordert, was den Umgang mit sensiblen Daten angeht? ☐ Ja ☐ Nein

2. Sind Ihnen aus den letzten 5 Jahren Netzwerksicherheitsverletzungen (wie Hacker-Angriffe, Denial-of-Service-Angriffe oder Vorfälle durch Schadprogramme), Bedienfehler, Datenrechtsverletzungen oder Cyber-Erpressungen o.ä. bekannt, die einen Schaden bei Ihnen oder einen Schadenersatzanspruch eines Dritten hervorgerufen haben oder sind Ihnen Umstände bekannt, die zu einem Cyber-Versicherungsfall führen könnte? ☐ Ja ☐ Nein

Wenn mindestens eine der beiden vorstehenden Fragen nicht mit „Nein“ beantwortet wurden, bitten wir um Details zu jedem Vorfall.

- Was ist konkret passiert (Detailbeschreibung)?
- Welche einzelnen Kosten sind Ihnen durch den Vorfall entstanden?
- Kam es zu einem Systemausfall/Betriebsausfall (vollständig oder teilweise), und wenn ja wie lange?
- Welche Maßnahmen wurden ergriffen um solche Vorfälle zukünftig möglichst zu vermeiden?

Datenschutz

Der Versicherungsnehmer willigt ein, dass der Versicherer im erforderlichen Umfang Daten, die sich aus den Antragsunterlagen oder der Vertragsdurchführung (Prämien, Versicherungsfälle, Risiko-/Vertragsänderungen) ergeben, an Rückversicherer sowie zur Beurteilung des Risikos und der Ansprüche an andere Versicherer/Gutachter/Rechtsanwälte etc. und/oder den HUK-Verband zur Weitergabe dieser Daten an andere Versicherer übermitteln darf. Diese Einwilligung gilt auch unabhängig vom Zustandekommen des Versicherungsvertrages sowie für entsprechende Prüfungen bei anderweitig beantragten Versicherungsverträgen und bei künftigen Anträgen. 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.

Name	Position im Unternehmen	Unterschrift Geschäftsleitung oder befugten Vertreters/Firmenstempel	Datum

Datenschutzerklärung

Hiscox verpflichtet sich, Ihre Privatsphäre zu schützen. Diese Datenschutzerklärung („Erklärung“) beschreibt die Einzelheiten zu den Daten, die wir von Ihnen verarbeiten, und wie wir diese Daten verarbeiten. Bitte nehmen Sie sich die Zeit, diese Erklärung sorgfältig durchzulesen. Wenn Sie eine Website von Hiscox nutzen, sollte dieser Hinweis zusammen mit den Website-Bedingungen gelesen werden.

Index

HISCOX

Datenschutzerklärung

I. Über uns

Hiscox ist ein internationales Versicherungsunternehmen. Wir bieten Versicherungen für Privatpersonen, Unternehmen und andere Versicherer an. Dies erreichen wir, indem wir Versicherungen sowohl selbst als auch bei anderen Versicherern anbieten.

Der Schutz Ihrer Privatsphäre sowie der Schutz Ihrer persönlichen Angaben ist uns ein wichtiges Anliegen. Wir werden unsere Datenschutzgrundsätze der Entwicklung des Datenschutzes und der Sicherheitstechnik kontinuierlich anpassen und weiter verbessern.

Um Ihnen ein Angebot machen und eine Versicherung anbieten zu können und um etwaige Ansprüche oder Beschwerden bearbeiten zu können, müssen wir Daten über Sie erheben und verarbeiten. Dies macht das jeweilige Hiscox-Unternehmen zum „Verantwortlichen". In dieser Erklärung verwenden wir die Begriffe „wir" oder „uns" oder „Hiscox" und beziehen uns auf das Unternehmen, das als Verantwortlicher für Ihre Informationen handelt.

Die datenschutzrechtlich verantwortliche Stelle für Deutschland ist die Hiscox SA, Niederlassung für Deutschland, Arnulfstraße 31, 80636 München. Wenn Sie Fragen haben, können Sie uns auch jederzeit per Telefon 0049 89 545801 100 oder per E-Mail an dataprotectionofficer@hiscox.com kontaktieren. Unter https://www.hiscox.de/datenschutz-unterrichtung/ finden Sie immer die aktuellste Fassung der vorliegenden Datenschutzerklärung.

II. Über den Versicherungsmarkt

Versicherung ist das Bündeln und Teilen von Risiken, um Schutz vor einer möglichen Eventualität zu bieten. Um dies zu erreichen, müssen Informationen, einschließlich Ihre personenbezogenen Daten, unter den verschiedenen Versicherungsmarktteilnehmern weitergegeben werden.

III. Welche personenbezogenen Daten erheben und verarbeiten wir?

Die personenbezogenen Daten, die wir erheben, hängen von Ihrer Beziehung zu uns ab. Wir erheben verschiedene personenbezogene Daten, abhängig davon, ob Sie Inhaber einer Hiscox-Police, ein Begünstigter gemäß einer Hiscox-Versicherungspolice, ein Anspruchsteller, ein Zeuge, ein Makler oder ein sonstiger Dritter sind.

Unter bestimmten Umständen können wir besondere Kategorien personenbezogener Daten (nachfolgend: „sensible personenbezogene Daten") über Sie anfordern und/oder erhalten. Beispielsweise könnten wir, falls es relevant ist, Zugriff auf Informationen über Ihre Gesundheit benötigen, um Ihnen ein Angebot zu machen, Ihnen Ihre Versicherungspolice bereitzustellen, oder um Ansprüche zu bearbeiten, die Sie erheben.

Wenn Sie uns personenbezogene Daten über andere Privatpersonen (z.B. Mitglieder Ihrer Familie) zur Verfügung stellen, erklären Sie, dass Sie die Privatperson über den Inhalt dieser Erklärung informieren und jede erforderliche Zustimmung für die Verarbeitung der personenbezogen Daten der Privatperson gemäß dieser Erklärung einholen werden.

Bitte klicken Sie auf den entsprechenden Abschnitt unten, um nähere Informationen über die Arten personenbezogener Daten zu erhalten, die wir unter verschiedenen Umständen wahrscheinlich über Sie erheben und verarbeiten werden.

Inhaber einer Police oder Begünstigter gemäß einer Versicherungspolice

Dieser Abschnitt gilt, wenn Sie eine Versicherungspolice direkt oder über einen bevollmächtigten Vermittler bei uns beantragen oder diese abschließen (z. B. eine Hausratspolice), oder wenn Sie als Antragsteller oder Begünstigter gemäß einer Police aufgeführt sind, die ein anderer bei uns abgeschlossen hat (z. B. ein benannter Fahrer bei einer Kfz-Police).

1. Personenbezogene Daten

   - Allgemeine Informationen, wie etwa Ihr Name, Ihre Adresse, Kontaktdaten, Geburtsdatum, Geschlecht und Beziehung zum Inhaber der Police (wenn Sie nicht der Inhaber der Police sind).

- Identifikationsangaben, wie etwa Sozialversicherungs-, Reisepass- oder Führerscheinnummer.
- Informationen über Ihren beruflichen Status, insbesondere Stellenbezeichnung, Ihren Status als Geschäftsführer oder Partner, beruflichen Werdegang, Ausbildungswerdegang und Berufszulassungen.
- Informationen, die für Ihre Versicherungspolice relevant sind, insbesondere Angaben von früheren Versicherungspolicen und Schadensverlauf. Dies hängt von der Art der Police ab, die Sie bei uns abschließen. Wenn Sie beispielsweise eine Hausrat- oder Gebäudeversicherung abschließen, können wir Informationen erheben und verarbeiten, die sich auf Ihr Eigentum beziehen, oder wenn Sie eine Vermögensschadenhaftpflichtversicherung abschließen, können wir Informationen erheben und verarbeiten, die sich auf berufliche Tätigkeit beziehen.
- Informationen, die für einen Anspruch, den Sie erheben, oder eine Beschwerde, die Sie einreichen, relevant sind. Dies hängt von der Art des erhobenen Anspruchs oder der eingereichten Beschwerde ab. Wenn Sie beispielsweise einen Anspruch nach einem Verkehrsunfall erheben, können wir personenbezogene Daten verarbeiten, die sich auf Ihr Fahrzeug und die benannten Fahrer beziehen.
- Finanzinformationen, wie etwa Ihre Bankverbindung, Zahlungsdaten und Informationen, die durch unsere Kreditprüfungen erhalten werden. Dies kann Einzelheiten zu Beschlüssen zur Eröffnung eines Konkursverfahrens, individuellen freiwilligen Vereinbarungen oder zu Gerichtsurteilen umfassen.
- Informationen (einschließlich Fotos), die wir aufgrund der Durchführung von Prüfungen öffentlich zugänglicher Quellen, wie Zeitungen und Social Media-Seiten, erhalten, zum Beispiel wenn wir betrügerische Aktivitäten vermuten oder diese für die Risikoeinschätzung relevant ist.
- Informationen, die wir aufgrund der Prüfung von Sanktionslisten erhalten.
- Informationen, wie etwa IP-Adresse und Browserverlauf, die wir aufgrund unserer Verwendung von Cookies erhalten. Weitere Informationen darüber erhalten Sie in unserer Cookie-Richtlinie, die Sie unter https://www.hiscox.de/datenschutzunterrichtung/ einsehen können.
- Informationen, die wir während Telefonaufzeichnungen erhalten haben.
- Ihre Marketing-Präferenzen und Einzelheiten zu Ihrer Kundenerfahrung mit uns.

2. Sensible personenbezogene Daten

- Informationen, die sich auf strafrechtliche Verurteilungen beziehen (einschließlich Straftaten, mutmaßlicher Straftaten und Gerichtsurteile oder nicht verbüßter Strafen).
- Falls relevant, Angaben zu Ihrem gegenwärtigen und früheren Gesundheitszustand.
- Unter bestimmten Umständen können wir weitere sensible personenbezogene Daten verarbeiten, einschließlich Angaben zu Ihrer Rasse, ethnischen Zugehörigkeit, Ihren religiösen oder philosophischen Überzeugungen, politischen Meinungen, Ihrer Gewerkschaftsmitgliedschaft, Ihren genetischen oder biometrischen Daten oder Angaben bezüglich Ihres Sexuallebens oder Ihrer sexuellen Orientierung, falls dies für Ihre Police oder Ihren Anspruch relevant ist. Wir können beispielsweise Informationen verarbeiten, die sich auf Ihre Gewerkschaftsmitgliedschaft beziehen, wenn Sie bei uns eine Police über Ihr Gewerkschaftsorgan abschließen, und wir können Informationen verarbeiten, die sich auf Ihre religiösen Überzeugungen beziehen, falls diese im Rahmen Ihrer medizinischen Behandlung relevant sind.

Drittanspruchsteller gemäß Hiscox-Versicherungspolice

Dieser Abschnitt gilt, wenn Sie einen Anspruch in Bezug auf einen Dritten erheben, der eine Hiscox-Versicherungspolice hat. Wenn Sie beispielsweise an einem Verkehrsunfall mit einem Dritten beteiligt sind, der bei uns versichert ist.

1. Personenbezogene Daten

- Allgemeine Informationen, wie etwa Ihr Name, Ihre Adresse, Kontaktdaten, Geburtsdatum und Geschlecht.
- Identifikationsangaben, wie etwa Ihre Sozialversicherungs-, Reisepass- oder Führerscheinnummer.
- Informationen über Ihre Arbeit, einschließlich Stellenbezeichnung, Ihres Status als Geschäftsführer oder Partner, beruflichen Werdegangs, Ausbildungswerdegangs und Berufszulassungen.
- Informationen, die für Ihren Anspruch relevant sind. Dies hängt von der Art des Anspruchs, den Sie erheben, ab. Wenn Sie beispielsweise einen Anspruch nach einem Verkehrsunfall erheben, können wir personenbezogene Daten verwenden, die sich auf Ihr Fahrzeug und die benannten Fahrer beziehen.
- Informationen, die sich auf frühere Versicherungspolicen oder Ansprüche beziehen.
- Finanzinformationen, wie etwa Ihre Bankverbindung und Zahlungsdaten.
- Informationen (einschließlich Fotos), die wir aufgrund der Durchführung von Prüfungen öffentlich zugänglicher Quellen, wie Zeitungen und Social Media-Seiten, erhalten, wenn wir betrügerische Aktivitäten vermuten.
- Informationen, die wir aufgrund der Prüfung von Sanktionslisten erhalten.
- Informationen, wie etwa IP-Adresse und Browserverlauf, die wir aufgrund unserer Verwendung von Cookies erhalten. Weitere Informationen darüber erhalten Sie in unserer Cookie-Richtlinie, die Sie unter https://www.hiscox.de/datenschutzunterrichtung/ einsehen können.
- Informationen, die wir während Telefonaufzeichnungen erhalten haben.

2 Sensible personenbezogene Daten

- Informationen, die sich auf Ihre strafrechtlichen Verurteilungen beziehen (einschließlich Straftaten, mutmaßlicher Straftaten und Gerichtsurteile oder nicht verbüßter Strafen aus strafrechtlichen Verurteilungen).
- Falls relevant, Angaben zu Ihrem gegenwärtigen und früheren Gesundheitszustand. Das kann zum Beispiel bei der Bearbeitung von Schadenersatzansprüchen gegenüber Versicherungsnehmern im Rahmen einer Betriebs- oder Privathaftpflichtversicherung erforderlich sein.
- Unter bestimmten Umständen können wir weitere sensible personenbezogene Daten verarbeiten, einschließlich Angaben zu Ihrer Rasse, ethnischen Zugehörigkeit, Ihren religiösen oder philosophischen Überzeugungen, politischen Meinungen, Ihrer Gewerkschaftsmitgliedschaft, Ihren genetischen oder biometrischen Daten oder Angaben bezüglich Ihres Sexuallebens oder Ihrer sexuellen Orientierung, falls dies für Ihren Anspruch relevant ist. Wir können beispielsweise Informationen verarbeiten, die sich auf Ihre religiösen Überzeugungen beziehen, falls diese im Rahmen Ihrer medizinischen Behandlung relevant sind.

Dritter gemäß einer gewerblichen Versicherungspolice oder einer Versicherungspolice, die wir einem anderen Versicherer anbieten

Dieser Abschnitt gilt, wenn Ihre Informationen in Bezug auf eine gewerbliche Versicherungspolice verarbeitet werden, die von einem Dritten unterhalten wird (z.B. wenn Sie ein Mitglied der Besatzung auf einem Schiff oder in einem Flugzeug sind, das wir versichern), oder wenn Ihre Informationen in Bezug auf eine Versicherungspolice verarbeitet werden, die wir einem anderen Versicherer anbieten.

1. Personenbezogene Daten

- Allgemeine Informationen, wie etwa Ihr Name, Ihre Adresse, Kontaktdaten, Geburtsdatum und Geschlecht.
- Identifikationsangaben, wie etwa Ihre Sozialversicherungs-, Reisepass- oder Führerscheinnummer.
- Informationen über Ihre Arbeit, einschließlich Stellenbezeichnung, Ihres Status als Geschäftsführer oder Partner, beruflichen Werdegangs, Ausbildungswerdegangs und Berufszulassungen.
- Informationen, die für einen erhobenen Anspruch relevant sind.
- Informationen, die sich auf frühere Versicherungspolicen oder Ansprüche beziehen.
- Finanzinformationen, wie etwa Ihre Bankverbindung und Zahlungsdaten.
- Informationen (einschließlich Fotos), die wir aufgrund der Durchführung von Prüfungen öffentlich zugänglicher Quellen, wie Zeitungen und Social Media--Seiten, erhalten, wenn wir betrügerische Aktivitäten vermuten.
- Informationen, die wir aufgrund der Prüfung von Sanktionslisten erhalten.
- Informationen, wie etwa IP-Adresse und Browserverlauf, die wir aufgrund unserer Verwendung von Cookies erhalten, die Sie unter https://www.hiscox.de/datenschutzunterrichtung/ einsehen können
- Informationen, die wir während Telefonaufzeichnungen erhalten haben.

2 Sensible personenbezogene Daten

- Informationen, die sich auf Ihre strafrechtlichen Verurteilungen beziehen (einschließlich Straftaten, mutmaßlicher Straftaten und Gerichtsurteile oder nicht verbüßter Strafen aus strafrechtlichen Verurteilungen).
- Falls relevant, Angaben zu Ihrem gegenwärtigen und früheren Gesundheitszustand.
- Unter bestimmten Umständen können wir weitere sensible personenbezogene Daten verarbeiten, einschließlich Angaben zu Ihrer Rasse, ethnischen Zugehörigkeit, Ihren religiösen oder philosophischen Überzeugungen, politischen Meinungen, Ihrer Gewerkschaftsmitgliedschaft, Ihren genetischen oder biometrischen Daten oder Angaben bezüglich Ihres Sexuallebens oder Ihrer sexuellen Orientierung, falls dies für die Police relevant ist. Wir können beispielsweise Informationen verarbeiten, die sich auf Ihre religiösen Überzeugungen beziehen, falls diese im Rahmen Ihrer medizinischen Behandlung relevant sind.

Zeugen bei einem Ereignis

Dieser Abschnitt gilt, wenn Sie Zeuge bei einem Ereignis sind, das Gegenstand eines Anspruchs ist.

1. Personenbezogene Daten

- Allgemeine Informationen, wie etwa Ihr Name, Ihre Adresse, Kontaktdaten, Geburtsdatum und Geschlecht.
- Identifikationsangaben, wie etwa Ihre Sozialversicherungs-, Reisepass- oder Führerscheinnummer.
- Informationen, die für das Ereignis, bei dem Sie Zeuge waren, relevant sind.

2. Sensible personenbezogene Daten

- Abhängig von der Art des Ereignisses, bei dem Sie Zeuge waren, und nur falls relevant, können wir Informationen, die sich auf Ihre strafrechtlichen Verurteilungen (einschließlich Straftaten, mutmaßlicher Straftaten und Gerichtsurteile oder nicht verbüßter Strafen aus strafrechtlichen Verurteilungen) beziehen, oder Angaben zu Ihrem gegenwärtigen oder früheren körperlichen oder geistigen Gesundheitszustand erfassen.
- Unter bestimmten Umständen können wir weitere sensible personenbezogene Daten verarbeiten, einschließlich Angaben zu Ihrer Rasse, ethnischen Zugehörigkeit, Ihren religiösen oder philosophischen Überzeugungen, politischen Meinungen, Ihrer Gewerkschaftsmitgliedschaft, Ihren genetischen oder biometrischen Daten oder Angaben bezüglich Ihres Sexuallebens oder Ihrer sexuellen Orientierung, falls dies für Ihre Rolle als Zeuge relevant ist.

Makler, ernannte Vertreter und sonstige Geschäftspartner

Dieser Abschnitt gilt, wenn Sie ein Makler, der mit uns Geschäfte macht, ein ernannter Vertreter oder ein sonstiger Geschäftspartner sind.

1. Personenbezogene Daten

- Allgemeine Informationen, wie etwa Ihr Name, Ihre Adresse, Kontaktdaten, Geburtsdatum und Geschlecht.
- Informationen über Ihre Arbeit, wie etwa Stellenbezeichnung, Ihr Status als Geschäftsführer oder Partner, beruflicher Werdegang, Ausbildungswerdegang und berufliche Akkreditierungen.
- Informationen, die wir aufgrund der Prüfung von Sanktionslisten erhalten.
- Sonstige Informationen (einschließlich öffentlich zugänglicher Informationen), die wir im Rahmen unserer Sorgfaltsprüfungen erhalten.

2 Sensible personenbezogene Daten

- Informationen, die sich auf Ihre strafrechtlichen Verurteilungen beziehen (einschließlich Straftaten, mutmaßlicher Straftaten und Gerichtsurteile oder nicht verbüßter Strafen aus strafrechtlichen Verurteilungen).

IV. Wie erheben wir Ihre Informationen?

Wir erheben personenbezogene Daten aus mehreren verschiedenen Quellen, z.B.:

- direkt von Ihnen;
- von sonstigen Dritten, die an der Verwaltung unserer Versicherungspolicen oder Ansprüche beteiligt sind (wie etwa unsere Geschäftspartner und Vertreter, Makler und andere Versicherer, Anspruchsteller, Beschuldigte oder Zeugen bei einem Ereignis);
- von sonstigen Dritten, die einen Dienst in Bezug auf unsere Versicherungspolicen oder Ansprüche anbieten (wie etwa Schadensregulierer, Anspruchssachbearbeiter, Sachverständige (einschließlich medizinischer Sachverständiger) und sonstige Dienstleister);
- von öffentlich zugänglichen Quellen, wie etwa Internetsuchmaschinen, Zeitungsartikeln und Social Media-Seiten;
- von anderen Unternehmen der Hiscox-Gruppe;
- von Kreditauskunfteien;
- von Ämtern und Datenbanken zur Erkennung von Finanzkriminalität (wie etwa zur Betrugsprävention und Prüfung auf internationale Sanktionen), einschließlich der Datenbank des Vereinigten Königreichs für Schadensfälle- und Versicherungsaustausch (Claims Underwriting Exchange, bekannt als „CUE“);

- von staatlichen Behörden, wie etwa der Polizei, der National Crime Agency (nationales Kriminalamt des Vereinigten Königreichs), der Kraftfahrzeugzulassungsstelle oder der britischen Steuerbehörde HMRC (Her Majesty's Revenue and Customs);
- von Dritten, die uns gegenüber Angaben zu Privatpersonen machen, die ein Interesse geäußert haben, etwas über Versicherungsprodukte zu erfahren;
- unter bestimmten Umständen von Privatdetektiven;
- von Drittanbietern von Daten (zum Beispiel in Bezug auf Flutmodellierungsdaten); und
- von unseren eigenen Websites.

V. Für welche Zwecke werden Ihre Informationen verarbeitet?

Wir können Ihre Informationen für verschiedene Zwecke verarbeiten. Für jeden Zweck müssen wir eine Rechtsgrundlage haben, um Ihre personenbezogenen Daten auf diese Weise zu verarbeiten.

Wenn die Informationen, die wir verarbeiten, als „sensible personenbezogene Daten" gilt, müssen wir einen spezielle zusätzliche Rechtsgrundlage haben, um diese Informationen zu verarbeiten.

In der Regel stützen wir uns auf die folgenden Rechtsgründe:

- Wir müssen Ihre personenbezogenen Daten verarbeiten, um einen Vertrag mit Ihnen abzuschließen oder einen Vertrag, den wir mit Ihnen geschlossen haben, zu erfüllen. Wir müssen beispielsweise Ihre personenbezogenen Daten verarbeiten, um Ihnen ein Angebot zu unterbreiten oder um Ihnen eine Versicherungspolice und andere zugehörige Produkte (z. B. Rechtsschutz-, Kfz-Haftpflichtversicherung) bereitzustellen. Wir stützen uns darauf bei Tätigkeiten wie der Bewertung Ihres Antrags, der Verwaltung Ihrer Versicherungspolice, der Abwicklung von Ansprüchen und wenn wir Ihnen andere Produkte anbieten.
- Wir haben eine rechtliche oder behördliche Verpflichtung, diese personenbezogenen Daten zu verarbeiten. Beispielsweise verlangen unsere Aufsichtsbehörden von uns, bestimmte Aufzeichnungen unseres Geschäftsumgangs mit Ihnen aufzubewahren.
- Wir müssen diese personenbezogenen Daten zur Geltendmachung, Ausübung oder Verteidigung unserer Rechtsansprüche verarbeiten. Dies kann der Fall sein, wenn wir vor Gericht verklagt wurden oder wenn wir selbst vor einem Gericht Klage erheben wollen.
- Es ist aus geschäftlichen Gründen notwendig, Ihre personenbezogenen Daten zu verarbeiten. Wir stützen uns darauf bei Tätigkeiten wie der Aufbewahrung unserer Geschäftsunterlagen, Schulungen und Qualitätssicherung und bei der Entwicklung und Verbesserung unserer Produkte und Dienstleistungen.
- Wir müssen Ihre personenbezogenen Daten aus Gründen des erheblichen öffentlichen Interesses verwenden. Es könnte beispielsweise notwendig sein, dass wir Untersuchungen zu betrügerischen Ansprüchen oder Geldwäsche durchführen müssen.
- Wenn Sie Ihre Einwilligung für unsere Verwendung Ihrer personenbezogenen Daten (z. B. in Bezug auf Ihre Marketing-Präferenzen) erteilt haben. Unter bestimmten Umständen benötigen wir Ihre Einwilligung, um sensible personenbezogene Daten (z. B. Gesundheitsinformationen) zu verarbeiten. Ohne sie können wir Ihnen möglicherweise Ihre Police nicht bereitstellen oder Ansprüche abwickeln. Wir werden immer erklären, warum Ihre Einwilligung notwendig ist.

Weitere Einzelheiten zu unseren „Rechtsgründen“ für jeden unserer Verarbeitungszwecke finden Sie nachstehend aufgelistet.

1. Um Prüfungen zur Betrugs-, Kredit- und Geldwäschebekämpfung durchzuführen.

   Rechtsgründe:

   - Die Verwendung ist notwendig, um einen Vertrag mit Ihnen abzuschließen oder einen Vertrag, den wir mit Ihnen geschlossen haben, zu erfüllen.
   - Es ist aus geschäftlichen Gründen notwendig, um Betrug und sonstige Finanzkriminalität zu verhindern.

   Rechtsgrund bei sensiblen personenbezogenen Daten:

   - Sie haben uns Ihre ausdrückliche Einwilligung erteilt. Wir benötigen Ihre Einwilligung, bevor wir Ihnen Ihre Police bereitstellen oder für Ihren Anspruch zahlen können.
   - Wir müssen Ihre Informationen verwenden, um unsere Rechtsansprüche geltend zu machen, auszuüben oder zu verteidigen.

2. Um Ihren Versicherungsantrag zu beurteilen und Ihnen ein Angebot zu unterbreiten.

   Rechtsgründe:

   - Die Verwendung ist notwendig, um einen Vertrag mit Ihnen abzuschließen oder einen Vertrag, den wir mit Ihnen geschlossen haben, zu erfüllen.
   - Es ist aus geschäftlichen Gründen notwendig, um Ihren Versicherungsantrag zu bewerten und das Antragsverfahren zu verwalten.

   Rechtsgrund bei sensiblen personenbezogenen Daten:

   - Sie haben uns Ihre ausdrückliche Einwilligung erteilt. Wir benötigen Ihre Einwilligung, bevor wir Ihnen Ihre Police bereitstellen können.

3. Verwaltung von Versicherungsansprüchen.

   Rechtsgründe:

   - Die Verwendung ist notwendig, um einen Vertrag mit Ihnen abzuschließen oder einen Vertrag, den wir mit Ihnen geschlossen haben, zu erfüllen.
   - Es ist aus geschäftlichen Gründen notwendig, um Ihren Anspruch zu bewerten und zu erfüllen sowie um das Anspruchsverfahren zu verwalten.

   Rechtsgrund bei sensiblen personenbezogenen Daten:

   - Sie haben uns Ihre ausdrückliche Einwilligung erteilt. Wir benötigen Ihre Einwilligung, bevor wir für Ihren Anspruch zahlen können.
   - Wir müssen Ihre Informationen verarbeiten, um unsere Rechtsansprüche geltend zu machen, auszuüben oder zu verteidigen.

4. Prävention und Untersuchung von Betrug. Dies könnte die Weitergabe Ihrer personenbezogenen Daten an Dritte, wie etwa die Polizei, andere Versicherungsunternehmen, Makler, Dienstleister, wie etwa Schadensregulierer, Ämter für Betrugsprävention und Datenbankanbieter sowie andere Finanzdienstleister beinhalten.

   Rechtsgründe:

   - Die Verwendung ist notwendig, um einen Vertrag mit Ihnen abzuschließen oder einen Vertrag, den wir mit Ihnen geschlossen haben, zu erfüllen.
   - Es ist aus geschäftlichen Gründen notwendig, um Betrug und sonstige Finanzkriminalität zu erkennen und zu verhindern.

   Rechtsgrund bei sensiblen personenbezogenen Daten:

   - Sie haben uns Ihre ausdrückliche Einwilligung erteilt. Wir benötigen Ihre Einwilligung, bevor wir Ihnen Ihre Police bereitstellen oder für Ihren Anspruch zahlen können.

- Wir müssen Ihre Informationen verarbeiten, um unsere Rechtsansprüche geltend zu machen, auszuüben oder zu verteidigen.

5. Kommunikation mit Ihnen und Beilegung von etwaigen Beschwerden von Ihnen.

Rechtsgründe:

- Die Verwendung ist notwendig, um einen Vertrag mit Ihnen abzuschließen oder einen Vertrag, den wir mit Ihnen geschlossen haben, zu erfüllen.
- Es ist aus geschäftlichen Gründen notwendig, um Ihnen Mitteilungen zu senden, Beschwerden zu erfassen und zu untersuchen und sicherzustellen, dass künftige Beschwerden ordnungsgemäß bearbeitet werden.

Rechtsgrund bei sensiblen personenbezogenen Daten:

- Sie haben uns Ihre ausdrückliche Einwilligung erteilt.
- Wir müssen Ihre Informationen verarbeiten, um unsere Rechtsansprüche geltend zu machen, auszuüben oder zu verteidigen.

6. Erfüllung unserer rechtlichen oder behördlichen Verpflichtungen.

Rechtsgründe:

- Wir müssen Ihre Informationen verarbeiten, um unsere rechtlichen Verpflichtungen zu erfüllen.

Rechtsgrund bei sensiblen personenbezogenen Daten:

- Sie haben uns Ihre ausdrückliche Einwilligung erteilt.
- Wir müssen Ihre Informationen verarbeiten, um unsere Rechtsansprüche geltend zu machen, auszuüben oder zu verteidigen.

7. Um einen Antrag für unsere eigene (Rück-)versicherung zu stellen und diese in Anspruch zu nehmen.

Rechtsgründe:

- Es ist aus geschäftlichen Gründen notwendig, um sicherzustellen, dass wir über eine angemessene Absicherung verfügen.

Rechtsgrund bei sensiblen personenbezogenen Daten:

- Sie haben uns Ihre ausdrückliche Einwilligung erteilt.
- Wir müssen Ihre Informationen verarbeiten, um unsere Rechtsansprüche geltend zu machen, auszuüben oder zu verteidigen.

8. Bei Versicherungsrisikomodellierung und Produkt- und Preisverbesserung.

Rechtsgründe:

- Es ist aus geschäftlichen Gründen notwendig (um die Produkte und Dienstleistungen, die wir anbieten, zu entwickeln und zu verbessern).

Rechtsgrund bei sensiblen personenbezogenen Daten:

- Sie haben uns Ihre ausdrückliche Einwilligung erteilt.

9. Bereitstellung verbesserter Qualität, von Schulungen und Sicherheit (zum Beispiel durch aufgezeichnete oder überwachte Telefonanrufe zu unseren Kontaktnummern oder Durchführung von Umfragen zur Kundenzufriedenheit).

Rechtsgründe:

- Es ist aus geschäftlichen Gründen notwendig, um die Produkte und Dienstleistungen, die wir anbieten, zu entwickeln und zu verbessern.

Zusätzlicher Rechtsgrund bei sensiblen personenbezogenen Daten:

- Sie haben uns Ihre ausdrückliche Einwilligung erteilt.

10. Verwaltung unserer Geschäftstätigkeit, wie etwa durch Führen von Buchhaltungsunterlagen, Durchführung einer Analyse der Finanzergebnisse, Verwendung von Informationen, um die internen Prüfanforderungen zu erfüllen und Inanspruchnahme von professioneller Beratung (z. B. Steuer- oder Rechtsberatung).

    Rechtsgründe:

    - Es ist aus geschäftlichen Gründen notwendig (um unseren Geschäftsbetrieb effektiv zu verwalten).

11. Bereitstellung von Marketing-Informationen für Sie entsprechend den Präferenzen, die Sie angegeben haben.

    Rechtsgründe:

    - Sie haben uns Ihre ausdrückliche Einwilligung erteilt.
    - Es ist aus geschäftlichen Gründen notwendig (um Ihnen ausgewählte Mitteilungen über Produkte und Dienstleistungen, die wir anbieten, zu senden).

VI. Wem geben wir Ihre Informationen weiter?

Gelegentlich können wir Ihre personenbezogenen Daten an die anderen Unternehmen der Hiscox-Gruppe oder an Dritte weitergeben. Wir behandeln Ihre personenbezogenen Daten vertraulich und geben Sie nur an Dritte weiter, die nachstehend für die in Abschnitt 5 erklärten Zwecke aufgelistet sind,.

Wenn Sie weitere Informationen bezüglich der Offenlegung Ihrer personenbezogenen Daten wünschen, kontaktieren Sie uns bitte unter Verwendung der nachstehend in Abschnitt 12 aufgeführten Angaben.

Offenlegung innerhalb der Hiscox-Gruppe

Wir können Ihre personenbezogenen Daten an andere Unternehmen innerhalb der Hiscox-Gruppe weitergeben, insbesondere wenn:

- eines unserer Gruppenunternehmen Ihre Police bei einem anderen Gruppenunternehmen platziert;
- eines unserer Gruppenunternehmen nicht in der Lage ist, Ihnen eine Versicherungspolice bereitzustellen, ein anderes jedoch in der Lage wäre, Ihnen behilflich zu sein;
- wir unsere eigene (Rück-)Versicherung abschließen;
- dies für unsere betriebswirtschaftlichen Zwecke notwendig ist;
- wir Informationen zur Prävention und Erkennung von Betrug oder sonstiger Kriminalität verwenden; oder
- wenn wir Informationen innerhalb unserer Unternehmensgruppe preisgeben müssen.

Offenlegungen gegenüber Dritten

Wir können Ihre personenbezogenen Daten gegenüber Dritten, die nachstehend aufgelistet sind, offenlegen, wenn dies für die in dieser Mitteilung beschriebenen Zwecke relevant ist. Dazu könnten gehören:

- unsere Versicherungs- und Rückversicherungspartner, wie etwa Makler, andere (Rück-)Versicherer oder andere Unternehmen, die als (Rück-)Versicherungsvermittler agieren;
- sonstige Dritte, die bei der Verwaltung Ihrer Versicherungspolice oder Ihres Anspruchs unterstützend tätig sind, wie etwa Schadensregulierer, Anspruchssachbearbeiter, Buchhalter, Rechnungsprüfer, Banken, Rechtsanwälte und sonstige Sachverständige, einschließlich medizinische Sachverständige;
- Unternehmen, die Ihnen bestimmte Dienstleistungen, wie etwa Versicherungsschutz für Haushaltsnotfälle, IT Sicherheit oder Rechtsschutzabdeckung bereitstellen;
- unsere Aufsichtsbehörden;

- Ämter zur Erkennung von Betrug und sonstige Dritte, die Register zur Erkennung von Betrug betreiben und unterhalten (einschließlich der Kraftfahrzeugversicherungsdatenbank) oder Untersuchungen bei vermutetem Betrug vornehmen;
- die Polizei und sonstige Dritte (wie etwa Banken oder andere Versicherungsunternehmen), wenn dies vernünftigerweise für die Prävention oder Erkennung von Kriminalität erforderlich ist;
- andere Versicherer, die unsere eigene Versicherung anbieten;
- Branchenverbände, wie etwa Gesamtverband der Deutschen Versicherungswirtschaft e.V., die Association of British Insurers (Verband der britischen Versicherer), Lloyd's Market Association (Marktverband von Lloyd's) oder das Employers' Liability Tracing Office (Amt zur Ermittlung der Arbeitgeberhaftpflicht);
- Kreditauskunfteien und Dritte, die Sanktionsprüfungen in unserem Auftrag durchführen;
- unsere Drittdienstleister, wie etwa IT-Anbieter, Aktuare, Rechnungsprüfer, Rechtsanwälte, Anbieter für Dokumentenmanagement und Postversand, Anbieter für ausgelagertes Geschäftsprozessmanagement, Contact und Service Center und Steuerberater;
- Dritte, die unser Direktmarketing in unserem Auftrag abwickeln (dazu gehört beispielsweise die Aufnahme oder das Löschen Ihrer personenbezogenen Daten in bzw. von unseren Kontaktlisten, das Versenden von Marketing-Mitteilungen und die Analyse der Reaktionen auf unsere Marketing-Mitteilungen);
- ausgewählte Dritte in Verbindung mit einem Verkauf, einer Übertragung oder Veräußerung unseres Unternehmens; oder
- falls erforderlich, Gerichte und andere Anbieter für alternative Streitbeilegung, wie etwa Schiedsrichter, Mediatoren und der Financial Ombudsman Service (britische Finanz--Ombudsstelle).

VII. Welche Marketingaktivitäten führen wir durch?

Wir können Ihre personenbezogenen Daten verarbeiten, um Ihnen Informationen über Produkte und Dienstleistungen bereitzustellen, die für Sie von Interesse sein könnten, wenn Sie ein Bestandskunde sind oder wenn Sie uns diesbezüglich Ihre Einwilligung erteilt haben.

Wir haben uns verpflichtet, Ihnen nur dann Marketing-Mitteilungen zu senden, wenn Sie ausdrücklich ein Interesse an deren Erhalt geäußert haben. Wenn Sie Marketingaktivitäten (wie z.B. den Newsletter) widerrufen möchten, können Sie dies tun, indem Sie auf den Link „Abbestellen" klicken, der in allen E-Mails erscheint, oder uns dies mitteilen, wenn wir Sie anrufen. Ansonsten können Sie uns jederzeit unter Verwendung der nachstehend in Abschnitt 12 aufgeführten Angaben kontaktieren, um Ihre Kontaktpräferenzen zu aktualisieren.

Bitte beachten Sie, selbst wenn Sie den Erhalt von Marketing-Nachrichten widerrufen, dass wir Ihnen gegebenenfalls weiterhin dienstleistungsbezogene Mitteilungen senden können.

VIII. Wie lange bewahren wir per--sonenbezogene Daten auf?

Wir bewahren Ihre personenbezogenen Daten nur solange auf, wie dies vernünftigerweise erforderlich ist, um die entsprechenden, in dieser Mitteilung dargelegten Zwecke zu erfüllen. Wir sind außerdem verpflichtet, bestimmte Informationen aufzubewahren, um unsere recht--lichen und behördlichen Verpflichtungen zu erfüllen.

Der genaue Zeitraum hängt von Ihrer Beziehung zu uns und der Art der personenbezogenen Daten, die wir haben, ab. Wenn Sie beispielsweise eine Versicherungspolice bei uns abschließen, bewahren wir Ihre personenbezogenen Daten länger auf, als wenn Sie ein Angebot von uns erhalten, jedoch keine Police abschließen.

Wenn Sie weitere Informationen bezüglich der Zeiträume, für die Ihre personenbezogenen Daten aufbewahrt werden, wünschen, kontaktieren Sie uns bitte unter Verwendung der in Abschnitt 12 aufgeführten Angaben.

IX. Wann versenden wir Informationen ins Ausland?

Wir (oder in unserem Auftrag handelnde Dritte) können Informationen aufbewahren oder verarbeiten, die wir über Sie in Ländern außerhalb des Europäischen Wirtschaftsraums („EWR“) erheben. Wenn wir eine Übermittlung Ihrer personenbezogenen Daten außerhalb des EWR vornehmen, treffen wir die erforderlichen Maßnahmen, um sicherzustellen, dass Ihre personenbezogenen Daten geschützt sind. Diese Schritte können sein, dass wir die Partei, an die wir die Informationen übermitteln, vertraglich verpflichten, Ihre personenbezogenen Daten nach angemessenen Standards zu schützen.

Wenn Sie weitere Informationen bezüglich der Maßnahmen wünschen, die wir treffen, um Ihre personenbezogenen Daten zu schützen, kontaktieren Sie uns bitte unter Verwendung der in Abschnitt 12 aufgeführten Angaben.

X. Wie schützen wir Ihre Informationen?

Wir verarbeiten eine Reihe von organisatorischen und technischen Sicherheitsmaßnahmen, um Ihre Informationen zu schützen, einschließlich Firewalls und Zugriffskontrollen, die wir in regelmäßigen Abständen überprüfen. Wir stellen ebenfalls sicher, dass unsere Mitarbeiter eine entsprechende Schulung zur Datensicherheit erhalten.

XI. Ihre Rechte

Nach dem Datenschutzrecht haben Sie bestimmte Rechte in Bezug auf die personenbezogenen Daten, die wir über Sie haben. Normalerweise wird keine Gebühr für die Bearbeitung dieser Anträge erhoben. Sie können diese Rechte jederzeit ausüben, indem Sie uns unter Verwendung der in Abschnitt 12 aufgeführten Angaben kontaktieren.

Bitte beachten Sie:

- Soweit gesetzlich zulässig, können wir Ihrem Antrag möglicherweise nicht entsprechen zum Beispiel, wenn der Antrag offenkundig unbegründet ist. Wir werden jedoch stets auf jedes von Ihnen gestellte Auskunftsersuchen reagieren, und wenn wir Ihrem Auskunftsersuchen nicht nachkommen können, werden wir Ihnen den Grund dafür nennen.
- Unter bestimmten Umständen bedeutet die Ausübung einiger dieser Rechte (einschließlich des Rechts auf Löschung, auf Einschränkung der Verarbeitung und auf Widerruf der Einwilligung), dass wir nicht in der Lage sind, Ihnen weiterhin eine Versicherung anzubieten, und kann daher in deren Stornierung resultieren. Sie verlieren daher möglicherweise das Recht, einen Anspruch geltend zu machen oder eine Leistung zu erhalten, einschließlich in Bezug auf ein Ereignis, das stattgefunden hat, bevor Sie Ihr Recht auf Löschung ausgeübt haben, wenn unsere Fähigkeit zur Abwicklung des Anspruchs beeinträchtigt wurde. Wir werden Ihnen dies zum Zeitpunkt mitteilen, zu dem Sie Ihre Einwilligung widerrufen möchten. Die Bedingungen Ihrer Police legen fest, was im Falle der Stornierung Ihrer Police passiert.

Ihre Rechte beinhalten:

1. Das Recht auf Auskunft über Ihre personenbezogenen Daten

   Sie haben das Recht auf eine Kopie der personenbezogenen Daten, die wir über Sie haben, und auf bestimmte Einzelheiten dazu, wie wir diese verwenden.

   Ihre Informationen werden Ihnen in der Regel schriftlich zur Verfügung gestellt, sofern nicht anders gewünscht oder wenn Sie die Anfrage auf elektronischem Wege gestellt haben, wobei Ihnen in diesem Fall die Informationen, soweit möglich, auf elektronischem Wege zur Verfügung gestellt werden.

2. Das Recht auf Berichtigung

   Wir treffen angemessene Maßnahmen, um sicherzustellen, dass die Informationen, die wir über Sie haben, richtig und vollständig sind. Wenn Sie jedoch der Ansicht sind, dass dies nicht der Fall ist, können Sie uns bitten, diese zu aktualisieren oder zu ändern.

3. Das Recht auf Löschung

   Unter bestimmten Umständen haben Sie das Recht, uns zu bitten, Ihre personenbezogenen Daten zu löschen, zum Beispiel, wenn die von uns erfassten personenbezogenen Daten nicht länger für den ursprünglichen Zweck benötigt werden, oder wenn Sie Ihre Einwilligung widerrufen. In gesetzlich bestimmten Fällen gilt das Recht auf Löschung nicht. Wir könnten beispielsweise rechtliche und behördliche Verpflichtungen haben, was bedeutet, dass wir Ihrer Anfrage nicht nachkommen können.

4. Das Recht auf Einschränkung der Verarbeitung

   Unter bestimmten Umständen haben Sie das Recht, uns zu bitten, die Verwendung Ihrer personenbezogenen Daten zu unterbinden, zum Beispiel, wenn Sie denken, dass die personenbezogenen Daten, die wir über Sie haben, falsch sind, oder wenn Sie denken, dass wir Ihre personenbezogenen Daten nicht länger benötigen.

5. Das Recht auf Datenübertragbarkeit

   Unter bestimmten Umständen haben Sie das Recht, uns zu bitten, personenbezogene Daten, die Sie uns bereitgestellt haben, Ihnen oder einem Dritten Ihrer Wahl zu übermitteln.

6. Das Recht auf Ablehnung von Marketing

   Sie können uns jederzeit bitten, aufzuhören, Ihnen Marketing-Nachrichten zu senden. Sie können dies tun, indem Sie entweder auf die Schaltfläche „Abbestellen“ in jeder E-Mail, die wir Ihnen senden, klicken, oder indem Sie uns unter Verwendung der in Abschnitt 12 aufgeführten Angaben kontaktieren. Bitte beachten Sie, selbst wenn Sie den Erhalt von Marketing-Nachrichten widerrufen, dass wir Ihnen gegebenenfalls weiterhin dienstleistungsbezogene Mitteilungen senden können.

7. Das Recht auf Widerspruch aus Gründen der besonderen persönlichen Situation

   Sie können aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung der Sie betreffenden personenbezogener Daten zum Zwecke der oben genannten geschäftlichen Gründe Widerspruch einlegen. Wir verarbeiten die personenbezogenen Daten dann nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

   Zur Ausübung Ihres Widerspruchsrechts kontaktieren Sie uns unter den in Abschnitt 12 aufgeführten Kontaktdaten.

8. Rechte in Bezug auf automatisierte Entscheidungsfindung

   Gelegentlich treffen wir Entscheidungen unter Verwendung von automatisierten Mitteln, wenn diese Entscheidung in Bezug auf Ihre Versicherungspolice notwendig ist. Der automatisierte Prozess prüft die Informationen, die Sie uns bereitstellen (zum Beispiel Angaben zum Eigentum, das Sie versichern möchten), sowie andere Informationen, wie etwa Postleitzahl und lokale Kriminalitätsrate, um zu bestimmen, ob Ihr Versicherungsantrag angenommen werden kann, und um die Höhe des Beitrags festzulegen.

   Wenn bei Ihnen eine automatisierte Entscheidung getroffen wurde und Sie mit dem Ergebnis nicht einverstanden sind, können Sie uns unter Verwendung der in Abschnitt 12 aufgeführten Angaben kontaktieren und uns bitten, die Entscheidung zu überprüfen.

   Wir treffen keine automatisierten Entscheidungen unter Verwendung Ihrer sensiblen personenbezogenen Daten, ohne Sie zuerst um Ihre Zustimmung zu bitten.

9. Das Recht auf Widerruf der Einwilligung ►

   Bei bestimmten Verarbeitungen Ihrer personenbezogenen Daten bitten wir Sie um Ihre Einwilligung. Wenn wir dies tun, haben Sie das Recht, Ihre Einwilligung für die weitere Verwendung Ihrer personenbezogenen Daten zu widerrufen. Durch Ihren Widerruf wird die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung nicht berührt.

   Bitte beachten Sie, dass wir für einige Zwecke Ihre Einwilligung benötigen, um Ihre Police bereitzustellen. Wenn Sie Ihre Einwilligung widerrufen, müssen wir möglicherweise Ihre Police stornieren bzw. können möglicherweise für Ihren Anspruch nicht zahlen. Wir werden Ihnen dies zum Zeitpunkt, zu dem Sie Ihre Einwilligung widerrufen möchten, mitteilen.

10. Das Recht, eine Beschwerde bei einer zuständigen Aufsichtsbehörde einzulegen ►

    Sie haben das Recht, bei einer zuständigen Aufsichtsbehörde (insb. derjenigen an Ihrem Aufenthaltsort, Arbeitsplatz oder dem Ort des Datenschutzverstoßes) Beschwerde einzulegen, wenn Sie glauben, dass eine Verarbeitung Ihrer personenbezogenen Daten durch uns gegen geltende Datenschutzbestimmungen verstößt.

    Das Einlegen einer Beschwerde schließt andere Rechtsansprüche oder Rechtsmittel, die Sie möglicherweise haben, nicht aus.

XII. Kontakt

Wenn Sie weitere Informationen über eines der Themen in dieser Mitteilung wünschen oder sonstige Fragen dazu haben, wie wir Ihre personenbezogenen Daten erheben, speichern oder in sonstiger Weise verarbeiten, können Sie uns per Telefon unter 0049 89 545801 100 kontaktieren oder uns eine E-Mail an dataprotectionofficer@hiscox.com senden .

Unseren bestellten Datenschutzbeauftragten erreichen Sie unter:

Daniel Kaiser
+49 89 545801100
dataprotectionofficer@hiscox.com

XIII. Aktualisierungen der Datenschutzerklärung

Von Zeit zu Zeit müssen wir Änderungen an der Datenschutzerklärung vornehmen, zum Beispiel aufgrund von gesetzlichen oder technologischen Änderungen oder anderen Entwicklungen. Sie sollten unsere Website https://www.hiscox.de/datenschutzunterrichtung/ regelmäßig besuchen, um die aktuellste Datenschutzerklärung einzusehen.

Diese Datenschutzerklärung wurde zuletzt aktualisiert am: 27.02.2018.