Drucken Zurücksetzen

Berkley Cyber Risk Protect

Cyber - Risikoerfassung für mittelständische Unternehmen

W. R. Berkley Europe AG – Niederlassung für Deutschland

Bitte beziehen Sie sich bei Ihren Angaben auf die Versicherungsnehmerin inkl. Tochtergesellschaften.

Stammdaten der Versicherungsnehmerin

Firmierung:		
Straße:	Postleitzahl:	Ort:
Mitarbeiteranzahl:	davon Mitarbeiter in der IT-Abteilung:	
Gründungsdatum:	Börsennotierung: ☐ Ja ☐ Nein	
Website:		

Tätigkeitsbeschreibung

Konsolidierte Finanzkennzahlen

konsolidierte Kennzahlen in EUR	Abgeschlossenes Geschäftsjahr in EUR	Prognose laufendes Geschäftsjahr in EUR
Umsätze insgesamt		
- davon in Deutschland/ Österreich		
- davon in der EU, EWR und Schweiz		
- davon in USA / Kanada		
- davon Rest der Welt		
- Onlineumsätze		
Bilanzsumme		
IT-Budget		

Tochtergesellschaften

Bitte listen Sie alle Tochtergesellschaften und Niederlassungen außerhalb der EU/ EWR auf (*ggf. bitte Zusatzblatt benutzen*):

Firmierung	Land	abweichende Tätigkeit zur VN

Anzahl von personenbezogenen Daten im Unternehmen

☐ 1 – 20.000 Datensätze
☐ 20.001 – 100.000 Datensätze
☐ 100.001 – 500.000 Datensätze
☐ 500.001 – 1.000.000 Datensätze
☐ über 1.000.000 Datensätze, nämlich ca. _____

Datenschutz

Es existiert eine schriftliche Datenschutzerklärung.	☐ Ja	☐ Nein
Die Datenschutzrichtlinie wurde durch einen externen Anwalt geprüft.	☐ Ja	☐ Nein
Es gibt einen unternehmensweiten Datenschutzbeauftragten (intern bzw. extern).	☐ Ja	☐ Nein
Alle Mitarbeiter sind im Umgang mit personenbezogenen Daten geschult bzw. haben eine Vertraulichkeitserklärung unterschrieben oder eine entsprechende Regelung in Ihrem Arbeitsvertrag.	☐ Ja	☐ Nein
Es gibt Zugangsberechtigungen für Benutzer zu personenbezogenen Daten inkl. regelmäßiger Überprüfung.	☐ Ja	☐ Nein
Personenbezogene Daten werden grundsätzlich verschlüsselt gespeichert „während dem Transit“ (z.B. E-Mail-Versand) als auch „at rest“ (Speicherung).	☐ Ja	☐ Nein
Die Vorschriften der DSGVO bzw. vergleichbarer Bestimmungen werden vollständig erfüllt.	☐ Ja	☐ Nein
Es gibt einen formalisierten Prozess und schriftliche Richtlinie, die die Aufbewahrung und das Löschen von personenbezogenen Daten regelt.	☐ Ja	☐ Nein
Es wurde innerhalb der letzten 12 Monate eine Datenschutzfolgeabschätzung vorgenommen.	☐ Ja	☐ Nein
Mobile Endgeräte, Festplatten und Wechseldatenträger sind grundsätzlich verschlüsselt. Der Verlust von mobilen Endgeräten muss unverzüglich dem Unternehmen angezeigt werden.	☐ Ja	☐ Nein

Physische Sicherheit: Serverraum/ Rechenzentrum

Es existieren geeignete Schutzmaßnahmen wie Einbruchschutz, Zutrittsberechtigungen, unterbrechungsfreie Stromversorgung, Notstrom, Klimatisierung, etc.	☐ Ja	☐ Nein

Risikomanagement

Es gibt regelmäßige Mitarbeiterschulungen und Trainings zum Thema Informationssicherheit, Datenschutz sowie Informationen über aktuelle Gefahrenpotentiale (z.B. aktuelle Trojaner, Phishing).	☐ Ja	☐ Nein
Es werden regelmäßige Phishing-Tests durchgeführt.	☐ Ja	☐ Nein
Es existiert eine unternehmensweite Sicherheitsrichtlinie bzw. Leitlinien im Umgang mit Informationssystemen, die an alle Mitarbeiter kommuniziert ist.	☐ Ja	☐ Nein
Es wurden unternehmenskritische Informationssysteme identifiziert und geeignete Kontrollinstrumente implementiert.	☐ Ja	☐ Nein
Ein Datenklassifizierungssystem ist vorhanden (Vertraulichkeit, Verfügbarkeit, Vollständigkeit).	☐ Ja	☐ Nein
Es besteht ein verpflichtendes 4-Augen-Prinzip bei Überweisungen/ Auszahlungen ab 25.000 EUR.	☐ Ja	☐ Nein
Es wurden geeignete Maßnahmen getroffen, um unautorisierte Warenlieferungen zu vermeiden.	☐ Ja	☐ Nein
Bei Telekommunikationsanlagen wurden voreingestellte Passwörter und Pins geändert.	☐ Ja	☐ Nein
Es besteht eine zwingende 2-Faktor Authentifizierung bei Anmeldung im Online-Banking und Überweisungsfreigabe.	☐ Ja	☐ Nein

IT-Schutzmaßnahmen

Auf allen IT-Systemen ist eine aktuelle Anti-Virus Software installiert, deren Aktualisierung zentral überwacht wird.	☐ Ja	☐ Nein
Es gibt einen formalisierten Prozess zum Aufspielen von Patches, Updates, Firmware, Software, etc. nach Herstellervorgaben.	☐ Ja	☐ Nein

Kritische Systemänderungen, Updates und Patches werden zuerst in einer Testumgebung geprüft, bevor diese in die „Live“-Umgebung eingespielt werden. Wie schnell werden kritische Patches unternehmensweit verteilt? _____	☐ Ja	☐ Nein
Es werden mindestens täglich vollständige Backups durchgeführt und regelmäßig geprüft – inkl. Wiederherstellungstest.	☐ Ja	☐ Nein
Backups sind vom Firmennetzwerk getrennt.	☐ Ja	☐ Nein
Backups sind verschlüsselt und die Verschlüsselung ist vom Netzwerk getrennt.	☐ Ja	☐ Nein
Es werden mehrere Backup-Strategien angewendet wie Cloud Backups und lokale Backups.	☐ Ja	☐ Nein
Die Integrität von Backups kann vor der Wiederherstellung getestet werden um sicher zu gehen, dass keine Malware vorhanden ist.	☐ Ja	☐ Nein
Es gibt eine schriftliche Passwort-Policy inkl. Vorgaben zur Komplexität und zeitlichen Gültigkeit (max. 90 Tage).	☐ Ja	☐ Nein
Zugangsberechtigungen basieren auf Anwenderrollen nach dem Prinzip der niedrigsten Berechtigung und es gibt einen Prozess der die Vergabe von Berechtigungen regelt.	☐ Ja	☐ Nein
Es gibt einen Prozess zur Einrichtung, Löschung, Sperrung oder Anpassung von Berechtigungen und Wiederherstellung von inventarisierten Informationen im Falle einer Einstellung bzw. Kündigung von Mitarbeitern oder internen Jobwechsel sowie bei einer Kündigung von externen Dritten, die Zugangsberechtigungen haben (z.B. Lieferanten).	☐ Ja	☐ Nein
Administrative Zugänge werden ausschließlich zur Erledigung administrativer Tätigkeiten genutzt. Für die alltägliche Nutzung (insbesondere Surfen im Internet und E-Mail-Kommunikation) wird ein Benutzer-Konto ohne Admin-Rechte verwendet.	☐ Ja	☐ Nein
Jeder Admin verwendet für administrative Tätigkeiten ausschließlich ein benutzerindividuelles Admin-Konto.		
Für PCs, Laptops, Server und mobile Endgeräte werden gesicherte Referenzkonfigurationen verwendet.	☐ Ja	☐ Nein
Es erfolgt eine Härtung der IT-Systeme durch die Löschung bzw. Deaktivierung von Softwarebestandteilen oder Funktionen, die nicht benötigt werden.	☐ Ja	☐ Nein
Mitarbeiter können ohne IT-Administratoren keine eigene Software installieren.	☐ Ja	☐ Nein
Es wurden geeignete Maßnahmen hinsichtlich der Verwendung von USB-Ports getroffen (automatische Verschlüsselung, Virenscan, Verbot zur Einbindung von Fremdhardware, etc.).	☐ Ja	☐ Nein
Mobile Endgeräte, Festplatten und Wechseldatenträgern sind grundsätzlich verschlüsselt.	☐ Ja	☐ Nein
Für mobile Endgeräte besteht die Möglichkeit zur Fernlöschung.	☐ Ja	☐ Nein
Spam-Filtering wird angewendet.	☐ Ja	☐ Nein
E-Mail Authentifizierung (SPF, DKIM, DMARC) ist durchgehend implementiert.	☐ Ja	☐ Nein
Externe Emails werden als solche gekennzeichnet.	☐ Ja	☐ Nein
Verwendung von Security Email Gateway (SEG).	☐ Ja	☐ Nein
Sandboxing zum Analysieren und Blockieren eingehender Email Anhänge mit bösartigem Anhang.	☐ Ja	☐ Nein
Mitarbeiter können verdächtige Emails als “Phishing-Angriff“ melden, die dann geprüft werden.	☐ Ja	☐ Nein

Netzwerksicherheit

Es existiert eine Firewall zwischen internem Netzwerk und dem Internet. Die Firewall wird regelmäßig angepasst und der Datenverkehr wird gefiltert und überwacht.	☐ Ja	☐ Nein
Es sind Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS) implementiert. Diese werden regelmäßig aktualisiert und überwacht.	☐ Ja	☐ Nein
Das Netzwerk ist segmentiert, sodass kritische Bereiche von weniger kritischen Bereichen getrennt sind.	☐ Ja	☐ Nein
Fernzugriffe auf das Firmennetzwerk und Cloud-Dienstleistungen erfolgen ausschließlich mit einer 2-Faktor-Authentifizierung.	☐ Ja	☐ Nein
Es wird eine regelmäßige Schwachstellenanalyse (Vulnerability Assessment) durchgeführt und, sofern notwendig, werden entsprechende Maßnahmen eingeleitet.	☐ Ja	☐ Nein
Es existiert ein Incident- und Change-Management.	☐ Ja	☐ Nein
Sicherheitsvorfälle wie Virus, Zugriffsversuche, Datenverluste etc. werden protokolliert und überwacht.	☐ Ja	☐ Nein
Der RDP-Port wurde deaktiviert.	☐ Ja	☐ Nein
Der SMB-Port wurde deaktiviert.	☐ Ja	☐ Nein
Eine EDR-Lösung (End Point Detection & Resposne) ist für alle kritischen Endpunkte und Server implementiert.	☐ Ja	☐ Nein
Bei allen End-Points sind die Administratorenrechte deaktiviert.	☐ Ja	☐ Nein

Multifaktor-Authentifizierung (MFA)

Die Multifaktor-Authentifizierung (MFA) ist für folgende Bereiche unternehmensweit implementiert:		
• Fernzugriff auf das Firmennetzwerk.	☐ Ja	☐ Nein
• Privilegierte/ Administratoren Benutzerkonten.	☐ Ja	☐ Nein
• Fernzugriff auf Cloud-basierte Anwendungen wie Office 365 oder Microsoft Azure.	☐ Ja	☐ Nein
• Fernzugriff auf E-Mails inkl. Cloud-basierter E-Mail-Systeme (sofern keine VPN-Verbindung genutzt wird).	☐ Ja	☐ Nein

Zertifizierungen

Wurden in den letzten 12 Monaten neue Zertifizierungen erreicht bzw. wurden vorhandene Zertifizierungen verlängert (z.B. ISO 27001, BSI Grundschutz)? *Falls ja, bitte Details:* ☐ Ja ☐ Nein

Outsourcing: Nutzung von externen IT-Dienstleistern, IT-Services und Cloud-Services

Überträgt Ihr Unternehmen IT- oder datenverarbeitungsbezogene Geschäftsaufgaben, Prozesse, Dienstleistungen (vollständig oder teilweise) an Dritte bzw. nutzt Cloud Services?	☐ Ja	☐ Nein
Es existiert eine schriftliche Outsourcing-Vereinbarung inkl. Sicherheitsanforderungen, die von diesem Dienstleister einzuhalten ist.	☐ Ja	☐ Nein
Es besteht ein Service Level Agreement (SLA) inkl. Vertragsstrafen, die bei Nichteinhaltung durch den Dienstleister zu zahlen sind.	☐ Ja	☐ Nein
Es bestehen keine Freistellungs- und/ oder haftungsbegrenzende Vereinbarungen mit den externen Dienstleistern.	☐ Ja	☐ Nein

Welche Bereiche wurden auf externe IT-Dienstleister und/ oder Cloud-Dienstleister ausgelagert und sind diese unternehmenskritisch? Bitte kurze Auflistung sowie **explizite** Nennung des entsprechenden Dienstleisters:

Dienstleister	Service	Unternehmenskritisch

Cyber-Krisenmanagement

Es existiert ein Krisenreaktionsplan mit folgenden Regelungen:

- Bei Störungen ist die Aufrechterhaltung bzw. der Wiederanlauf von betriebsnotwendigen Systemen festlegt. ☐ Ja ☐ Nein
- Kommunikationsplan für Betroffene. ☐ Ja ☐ Nein
- Feste Aufgabenverteilung für die Behandlung des Vorfalls im Unternehmen. ☐ Ja ☐ Nein
- Alternative Outsourcing-Kapazitäten für den Fall eines Ausfalls eines Outsourcing Dienstleisters im Bereich unternehmenskritischer Bereiche. ☐ Ja ☐ Nein
- Die Kontaktdaten der Cyber-Krisenhotline von W. R. Berkley und das Vorgehen zur Schadenmeldung werden in den Krisenreaktionsplan übernommen. ☐ Ja ☐ Nein

Es existiert ein Business Continuity Plan (BCP). ☐ Ja ☐ Nein

Es existiert eine Notfall-/ Disaster Recovery Plan (DRP). ☐ Ja ☐ Nein

Der Krisenreaktionsplan, Business Continuity Plan (BCP) und/oder der Notfall-/ Disaster-Recovery Plan (DRP) wird regelmäßig getestet und aktualisiert. ☐ Ja ☐ Nein

Operations Technology (OT)

Wie schnell führt eine Nichtverfügbarkeit Ihrer Systeme zu signifikanten Auswirkungen auf Ihre Geschäftstätigkeit?

Sofort ☐ nach 6h ☐ nach 12h ☐ nach 24h ☐ nach 48h ☐

Die fortlaufende Produktion / Logistik ist bei einem Ausfall der IT-Systeme vollständig manuell und offline möglich. ☐ Ja ☐ Nein

- Falls ja: Über welchen Zeitraum, bevor der Geschäftsbetrieb zu einem kompletten Stilstand kommt?_____
- Wie würden die Produktion und die Logistik in diesem Fall fortgeführt? _____
- Ist dieses Notfall-Szenario bereits getestet worden? ☐ Ja ☐ Nein

Bei einem IT-bedingten Ausfall der Produktion kann auf ein Lager an Fertigprodukten zurückgegriffen werden. ☐ Ja ☐ Nein

- Falls ja, über welchen Zeitraum ist dies möglich, bevor es zu Lieferengpässen, bis hin zu einem kompletten Stillstand bei der Auslieferung kommt? _____

Folgende Schutzmassnahmen sind durchgehend implementiert:

- Fernzugriffe sind nicht möglich. ☐ Ja ☐ Nein
- Schnittstellen an Terminals sind deaktiviert. ☐ Ja ☐ Nein
- OT befindet sich in einem separierten Netzwerk. ☐ Ja ☐ Nein
- Zugriffsrechte bestehen ausschließliche für die entsprechenden User. ☐ Ja ☐ Nein
- Fernzugriffe erfordern eine VPN-Verbindung. ☐ Ja ☐ Nein
- Fernzugriffe erfordern MFA. ☐ Ja ☐ Nein

• Fernzugriffe werden durchgehend protokolliert.	☐ Ja	☐ Nein
• Kontinuierliche Überwachung und bedarfsgerechte An-/ Abschaltung von Fernzugriffen.	☐ Ja	☐ Nein
• Externe Wartungszugänge sind besonders gesichert (Freigabe, etc.).	☐ Ja	☐ Nein

Remote/ außerhalb des Büros arbeiten

Es wird sichergestellt, dass die IT-Sicherheitsmaßnahmen und Datenschutzregelungen auch remote eingehalten werden.	☐ Ja	☐ Nein
Es gibt eine schriftliche Richtlinie/ Anleitung/ festgelegte Vorgehensweise für Mitarbeiter die remote arbeiten. In diesem Zusammenhang gibt es eine Regelung zur IT-Sicherheit und zum Umgang mit elektronischen und physischen Daten.	☐ Ja	☐ Nein
Die Verbindung zum Firmennetzwerk erfolgt ausschließlich über abgesicherte Zugangsmöglichkeiten (VPN, Citrix, VDI, etc.).	☐ Ja	☐ Nein
Alle Endgeräte verfügen über ein aktuelles Betriebssystem und Endpoint Protection.	☐ Ja	☐ Nein
Infolge des remote Arbeitens kommt es zu keiner Einschränkung bei:		
• IDS/ IPS	☐ Ja	☐ Nein
• Malware- und Virenerkennung	☐ Ja	☐ Nein
• Datensicherungen	☐ Ja	☐ Nein
• EDR-Tools	☐ Ja	☐ Nein
• Patchmanagement	☐ Ja	☐ Nein
Mitarbeiter nutzen ausschließlich Firmengeräte und **keine** „bring your own device“ Geräte.	☐ Ja	☐ Nein
Fernzugriffe auf das Firmennetzwerk und Cloud-Dienstleistungen erfolgen ausschließlich mit einer 2-Faktor-Authentifizierung.	☐ Ja	☐ Nein

End-of-life, end-of-Service, Legacy Systeme

Es werden **keine** End-of-life (EoL), end-of-Service (EoS) oder Legacy Systeme verwendet?	☐ Ja	☐ Nein
Falls doch, wurden folgende Schutzmaßnahmen implementiert:		
• Es erfolgt eine kontinuierliche Bestandsaufnahme und Überprüfung nach Kritikalität von EOL/EOS-Assets.	☐ Ja	☐ Nein
• Es gibt einen Migrationsplan. Wenn ja: bis _____	☐ Ja	☐ Nein
• Es wird ein verlängerter Herstellersupport verwendet.	☐ Ja	☐ Nein
• Betrieb in einem separierten Netzwerk.	☐ Ja	☐ Nein
• Es besteht kein direkter Internetzugang.	☐ Ja	☐ Nein
• Durchgehende Kontrolle des Datenverkehrs.	☐ Ja	☐ Nein

Elektronischer Zahlungsverkehr (Payment Card Industry)

Speichert, verarbeitet oder übermittelt Ihr Unternehmen bzw. ein externer Dienstleister Kreditkartendaten?	☐ Ja	☐ Nein
Es wird der aktuell geltende Payment Card Industry Data Security Standard (PCI DSS) im Unternehmen bzw. beim Dienstleister eingehalten.	☐ Ja	☐ Nein
Durchschnittliches Transaktionsvolumen und abgewickelte Zahlungen pro Jahr in EUR:_____		
Die Speicherung, Verarbeitung oder Übermittlung von Kreditkartendaten wurde an einen zertifizierten Dienstleister ausgelagert. Name des externen Dienstleisters: _____	☐ Ja	☐ Nein
PCI Level: Level 1 ☐ Level 2 ☐ Level 3 ☐ Level 4 ☐		

Schadenhistorie und bekannte Umstände in Bezug auf die Cyber-Versicherung

Sind Ihnen aus den letzten 5 Jahren Umstände, Inanspruchnahmen, Beschwerden oder Schäden bekannt, die zu einem Versicherungsfall unter den Versicherungsschutz dieser Cyber-Versicherung führen könnten? ja nein

Dies sind u.a. Hacker-Angriffe, interne/ externe Ermittlungen und Untersuchungen in Bezug auf Datenschutzverletzungen, Vorfälle durch Schadprogramme, Cyber-Erpressungen, Bedienfehler, technische Probleme, Datenverluste, ungeplante Betriebsunterbrechungen sowie Schadenersatzansprüche von Dritten in Bezug auf Datenrechtsverletzungen oder drohenden/ anhängigen Verfahren von Datenschutzbehörden.

Bitte listen Sie alle tatsächlichen oder potentiellen Umstände/ Schäden inklusive Beschreibung auf. (*insbesondere Datum; Beschreibung der Umstände; Beschreibung der getroffenen Gegenmaßnahmen; Finanzieller Aufwand/ Schaden*):

HINWEIS

Die Versicherungsnehmerin willigt ein, dass der Versicherer im erforderlichen Umfang Daten, die sich aus den Antragsunterlagen oder der Vertragsdurchführung (Prämien, Versicherungsfälle, Risiko-/Vertragsänderungen) ergeben, an Rückversicherer und Unternehmen der Berkley Gruppe sowie falls erforderlich an (externe) Dienstleister zur Beurteilung des Risikos und der Ansprüche an andere Versicherer/Gutachter/Rechtsanwälte/ Krisendienstleister etc. übermitteln darf. Diese Einwilligung gilt auch unabhängig vom Zustandekommen des Versicherungsvertrages sowie für entsprechende Prüfungen bei anderweitig beantragten Versicherungsverträgen und bei künftigen Anträgen.
Mit Ihrer Unterschrift bestätigen Sie, dass vorstehende Angaben vollständig und richtig sind.

Unsere aktuelle Datenschutzerklärung finden Sie unter: http://www.berkleyversicherung.de/datenschutz/

Bitte beachten Sie die gesonderte Mitteilung über die Folgen einer Verletzung der vorvertraglichen Anzeigepflicht im Anschluss an diesen Fragebogen.

_____	_____	_____
Ort, Datum	Unterschrift eines Repräsentanten der Versicherungsnehmerin i.S.d. Versicherungsbedingungen	Firmenstempel

Gesonderte Mitteilung über die Folgen einer Verletzung der vorvertraglichen Anzeigepflicht

Gemäß § 19 Absatz 1 VVG hat der Versicherungsnehmer

„bis zur Abgabe seiner Vertragserklärung die ihm bekannten Gefahrumstände, die für den Entschluss des Versicherers, den Vertrag mit dem vereinbarten Inhalt zu schließen, erheblich sind und nach denen der Versicherer in Textform gefragt hat, dem Versicherer anzuzeigen. Stellt der Versicherer nach der Vertragserklärung des Versicherungsnehmers, aber vor Vertragsannahme Fragen im Sinn des Satzes 1, ist der Versicherungsnehmer auch insoweit zur Anzeige verpflichtet."

Gemäß § 19 Absatz 5 Seite 1 VVG stehen dem Versicherer Rechte wegen einer Verletzung

der vorvertraglichen Anzeigepflicht nur zu, „wenn er den Versicherungsnehmer durch gesonderte Mitteilung in Textform auf die Folgen einer Anzeigepflichtverletzung hingewiesen hat."

Deshalb weisen wir Sie auf die nachstehenden gesetzlichen Regelungen über die Folgen einer Anzeigepflichtverletzung hin:

§ 19 VVG (Anzeigepflicht)

(2) Verletzt der Versicherungsnehmer seine Anzeigepflicht nach Absatz 1, kann der Versicherer vom Vertrag zurücktreten.

(3) Das Rücktrittsrecht des Versicherers ist ausgeschlossen, wenn der Versicherungsnehmer die Anzeigepflicht weder vorsätzlich noch grob fahrlässig verletzt hat. In diesem Fall hat der Versicherer das Recht, den Vertrag unter Einhaltung einer Frist von einem Monat zu kündigen.

(4) Das Rücktrittsrecht des Versicherers wegen grob fahrlässiger Verletzung der Anzeigepflicht und sein Kündigungsrecht nach Absatz 3, Satz 2 sind ausgeschlossen, wenn er den Vertrag auch bei Kenntnis der nicht angezeigten Umstände, wenn auch zu anderen Bedingungen, geschlossen hätte. Die anderen Bedingungen werden auf Verlangen des Versicherers rückwirkend, bei einer vom Versicherungsnehmer nicht zu vertretenden Pflichtverletzung ab der laufenden Versicherungsperiode Vertragsbestandteil.

(5) Dem Versicherer stehen die Rechte nach den Absätzen 2 bis 4 nur zu, wenn er den Versicherungsnehmer durch gesonderte Mitteilung in Textform auf die Folgen einer Anzeigepflichtverletzung hingewiesen hat. Die Rechte sind ausgeschlossen, wenn der Versicherer den nicht angezeigten Gefahrumstand oder die Unrichtigkeit der Anzeige kannte.

(6) Erhöht sich im Fall des Absatzes 4, Satz 2 durch eine Vertragsänderung die Prämie um mehr als zehn Prozent oder schließt der Versicherer die Gefahrabsicherung für den nicht angezeigten Umstand aus, kann der Versicherungsnehmer den Vertrag innerhalb eines Monats nach Zugang der Mitteilung des Versicherers ohne Einhaltung einer Frist kündigen. Der Versicherer hat den Versicherungsnehmer in der Mitteilung auf dieses Recht hinzuweisen.

§ 20 VVG (Vertreter des Versicherungsnehmers)

Wird der Vertrag von einem Vertreter des Versicherungsnehmers geschlossen, sind bei der Anwendung des § 19 Absatz 1 bis 4 und des § 21 Absatz 2 Satz 2 sowie Absatz 3 Satz 2 sowohl die Kenntnis und die Arglist des Vertreters als auch die Kenntnis und die Arglist des Versicherungsnehmers zu berücksichtigen. Der Versicherungsnehmer kann sich darauf, dass die Anzeigepflicht nicht vorsätzlich oder grob fahrlässig verletzt worden ist, nur berufen, wenn weder dem Vertreter noch dem Versicherungsnehmer Vorsatz oder grobe Fahrlässigkeit zu Last fällt.

§ 21 VVG (Ausübung der Rechte des Versicherers)

(1) Der Versicherer muss die ihm nach § 19 Absatz 2 bis 4 zustehenden Rechte innerhalb eines Monats schriftlich geltend machen. Die Frist beginnt mit dem Zeitpunkt, zu dem der Versicherer von der Verletzung der Anzeigepflicht, die das von ihm geltend gemachte Recht begründet, Kenntnis erlangt. Der Versicherer hat bei der Ausübung seiner Rechte die Umstände anzugeben, auf die er seine Erklärung stützt; er darf nachträglich weitere Umstände zur Begründung seiner Erklärung angeben, wenn für diese die Frist nach Satz 1 nicht verstrichen ist.

(2) Im Fall eines Rücktritts nach § 19 Absatz 2 nach Eintritt des Versicherungsfalles ist der Versicherer nicht zur Leistung verpflichtet, es sei denn, die Verletzung der Anzeigepflicht bezieht sich auf einen Umstand, der weder für den Eintritt oder die Feststellung des Versicherungsfalles noch für die Feststellung oder den Umfang der Leistungspflicht des Versicherers ursächlich ist. Hat der Versicherungsnehmer die Anzeigepflicht arglistig verletzt, ist der Versicherer nicht zur Leistung verpflichtet.

(3) Die Rechte des Versicherers nach § 19 Absatz 2 bis 4 erlöschen nach Ablauf von fünf Jahren nach Vertragsschluss; dies gilt nicht für Versicherungsfälle, die vor Ablauf dieser Frist eingetreten sind. Hat der Versicherungsnehmer die Anzeigepflicht vorsätzlich verletzt, beläuft sich die Frist auf zehn Jahre.

§ 22 VVG (Arglistige Täuschung)

Das Recht des Versicherers, den Vertrag wegen arglistiger Täuschung anzufechten, bleibt unberührt.