Drucken Zurücksetzen

Berkley Cyber Risk Protect

Risikoerfassung für mittelständische Unternehmen bis 300 MEUR konsolidierter Jahresumsatz

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

Stammdaten zur Versicherungsnehmerin

Firmierung:			
Straße:	Postleitzahl:	Ort:	
Anzahl an Mitarbeitenden:	Mitarbeitende in der IT-Abteilung:		
Davon Mitarbeitende mit PC-Arbeitsplatz:			
Gründungsdatum:	Börsennotierung:	☐ Ja	☐ Nein
Website(s):	Branche:		

Betriebs-/ Produktbeschreibung

Finanzkennzahlen

Bitte die (konsolidierten) Kennzahlen in EUR angeben	**Prognose lfd. Geschäftsjahr**	**Letztes Geschäftsjahr 20**
Umsätze insgesamt		
• davon in Deutschland/ Österreich		
• davon in der EU, EWR und Schweiz		
• davon in USA / Kanada		
• davon Rest der Welt		
• Onlineumsätze/ e-commerce (über eigene Website generiert)		
Bilanzsumme (insbesondere bei Finanzdienstleister)		
Bruttojahresgewinn		
Rohertrag (Umsatz abzüglich Materialkosten/ Einkaufspreis)		
IT-Budget		

Tochtergesellschaften

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

Firmierung	**Land**	**Umsatz**	**Abweichende Tätigkeit zur VN**

Anzahl personenbezogener 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	☐ Andere:

Nutzen Sie bei den **Ja-/Nein-Fragen** gerne die pdf-Kommentar-Funktion, wenn Sie uns etwas mitteilen möchten. So geht's: Im pdf rechte Maustaste klicken, "Kommentar hinzufügen" auswählen, Kommentar schreiben, "Beitragen" auswählen, Fenster schließen und den Kommentar-Icon mit der Maus an die entsprechende Stelle im Fragebogen ziehen.

Datenschutz

Es existiert eine schriftliche Datenschutzrichtlinie.	☐ Ja	☐ Nein
Die Datenschutzrichtlinie wird jährlich auf Konformität zu den geltenden Datenschutzregeln überprüft und notwendige Anpassungen zeitnah umgesetzt.	☐ Ja	☐ Nein
Es gibt einen unternehmensweiten Datenschutzbeauftragten (intern bzw. extern).	☐ Ja	☐ Nein
Vertrauliche Daten und personenbezogene Daten werden verschlüsselt:		
a) bei der Speicherung	☐ Ja	☐ Nein
b) bei der Übertragung (intern und extern)	☐ Ja	☐ Nein
Die Vorschriften der DSGVO bzw. vergleichbarer Bestimmungen werden vollständig erfüllt.	☐ Ja	☐ Nein
Informationen werden nach Schutzzielanforderungen (Vertraulichkeit, Integrität, Verfügbarkeit) klassifiziert.	☐ Ja	☐ Nein
Es wurde innerhalb der letzten 12 Monate eine Datenschutzfolgeabschätzung vorgenommen.	☐ Ja	☐ Nein
Mobile Endgeräte, Festplatten und Wechseldatenträger sind grundsätzlich verschlüsselt.	☐ Ja	☐ Nein
Der Verlust von Firmenhardware muss unverzüglich dem Unternehmen angezeigt werden.	☐ Ja	☐ Nein
Es ist eine Mobile Device Management-Lösung (MDM) implementiert und es ist möglich die Daten auf den mobilen Geräten aus der Ferne zu löschen.	☐ Ja	☐ Nein
Ihre Kommentare:		

Physische Sicherheit: Serverraum/Rechenzentrum

Kritische Systeme sind redundant ausgelegt (Aktiv-/Aktiv- oder Passiv-/Passiv- Architektur).	☐ Ja	☐ Nein
Für kritische Systeme sind eine unterbrechungsfreie Stromversorgung und Klimatisierung vorhanden.	☐ Ja	☐ Nein
Die unterbrechungsfreie Stromversorgung wird jährlich gewartet und getestet.	☐ Ja	☐ Nein
Physische Zugangskontrollen für Rechenzentren und Serverräume sind vorhanden.	☐ Ja	☐ Nein
Ihre Kommentare:		

Risikomanagement

Es gibt regelmäßige (mind. jährliche) Mitarbeiterschulungen/Trainings zum Thema Informationssicherheit, Datenschutz sowie Informationen über aktuelle Gefahrenpotenziale (z.B. Trojaner, Phishing, Ransomware).	☐ Ja	☐ Nein
Es werden regelmäßige Phishing-Tests durchgeführt. Wenn ja, bitte Information zur Häufigkeit.	☐ Ja	☐ Nein
Mitarbeitende können verdächtige E-Mails als „Phishing-Angriff" zur Prüfung melden.	☐ 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
Es besteht eine zwingende 2-Faktor Authentifizierung bei Anmeldung im Online-Banking und bei Überweisungsfreigaben.	☐ Ja	☐ Nein
Die identifizierten Schwachstellen werden in Anhängigkeit der Kritikalität behoben.	☐ Ja	☐ Nein
Ihr Unternehmen erhält regelmäßig Informationen zu Bedrohungen, Sicherheitslücken, Schwachstellen.	☐ Ja	☐ Nein
Ihre Kommentare:		

IT-Schutzmaßnahmen

Auf allen IT-Systemen ist eine aktuelle Anti-Virus Software installiert, deren Aktualisierung zentral überwacht wird.	☐ Ja	☐ Nein
Es gibt eine kontinuierliche Bestandsaufnahme der eingesetzten Soft-/ Hardware inkl. Schwachstellenanalyse.		
Es gibt einen zentralen/automatisierten Prozess zum Aufspielen von Patches, Updates, Firmware, Software, etc. nach Herstellervorgaben.	☐ Ja	☐ Nein
Patches/ Updates/ kritische Sicherheitslücken mit CVSs Score ab 7,0 bzw. BSI Bedrohungslage „orange und/oder „rot“ werden unverzüglich (72 Stunden) nach Herstellervorgaben geschlossen bzw. die empfohlen Maßnahmen werden umgesetzt. Alternative Dauer der Einspielung:	☐ Ja	☐ Nein
Patch-/ Updateinstallationen können durch den Benutzer nicht oder nur stark begrenzt (max. 12h) aufgeschoben werden.	☐ Ja	☐ Nein
Es werden mindestens täglich vollständige Backups durchgeführt.	☐ Ja	☐ Nein
Backups werden regelmäßig (mind. quartalsweise) geprüft – inkl. Wiederherstellungstest.	☐ Ja	☐ Nein
Backups sind vom Firmennetzwerk getrennt.	☐ Ja	☐ Nein
Backups sind verschlüsselt oder unveränderlich (immutable).	☐ Ja	☐ Nein
Es werden mehrere Backup-Strategien angewendet wie z.B. Cloud Backups und lokale Backups.	☐ Ja	☐ Nein
Der Zugriff auf Backups erfolgt mittels Authentifizierungsmechanismus außerhalb des Active Directory.	☐ Ja	☐ Nein
Die Integrität von Backups kann vor der Wiederherstellung getestet werden, um Malware auszuschließen.	☐ Ja	☐ Nein
Es gibt eine schriftliche Passwort-Policy inkl. Vorgaben zur Komplexität analog aktueller Empfehlungen (z.B. BSI). Alternativ wird dies technisch erzwungen.	☐ Ja	☐ Nein
Sämtliche Standard-/Initial-Passwörter wurden geändert und durch komplexe Passwörter ersetzt.	☐ Ja	☐ Nein
Zugangsberechtigungen sind individualisiert und basieren auf Anwenderrollen nach dem Prinzip “need to know“ 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 der Einstellung/Kündigung von Mitarbeitern, internen Jobwechseln sowie bei Kündigung externer Dritter mit Zugangsberechtigungen (z.B. Lieferanten bzw. Fernwartungszugänge).	☐ Ja	☐ Nein
Administrative Zugänge/ privilegierte Benutzerkonten werden ausschließlich zur Erledigung dieser Tätigkeiten genutzt. Für die alltägliche Nutzung (insbesondere Surfen im Internet, Email-Kommunikation) wird ein Benutzer-Konto ohne Admin-/ privilegierte-Rechte verwendet.	☐ Ja	☐ Nein
Für PCs, Laptops, Server und mobile Endgeräte werden gesicherte Referenzkonfigurationen verwendet.	☐ Ja	☐ Nein
Es wurden geeignete Maßnahmen hinsichtlich der Verwendung von USB-Ports getroffen (automatische Verschlüsselung, Virenscan, Verbot zur Einbindung von Fremdhardware, etc.).	☐ Ja	☐ Nein
Die Authentifizierung (SPF, DKIM, DMARC) ist durchgehend implementiert.	☐ Ja	☐ Nein
Externe Emails werden als solche gekennzeichnet.	☐ Ja	☐ Nein
Einsatz von Security Email Gateway (SEG).	☐ Ja	☐ Nein
Einsatz von Sandboxing zum Analysieren und Blockieren eingehender Email Anhänge, die als bösartig bzw. nicht vertrauenswürdig eingestuft werden.	☐ Ja	☐ Nein
Accounts werden nach einer bestimmten Anzahl an ungültigen Anmeldeversuchen temporär gesperrt.	☐ Ja	☐ Nein
Ihre Kommentare:		

Netzwerksicherheit

Es existiert eine Firewall zwischen internem Netzwerk und Internet. Die Firewall wird kontinuierlich aktualisiert und angepasst, sowie der Datenverkehr gefiltert und überwacht.	☐ Ja	☐ Nein
Firewall-Logdaten werden mindestens 90 Tage gespeichert.	☐ Ja	☐ Nein
Es sind Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS) implementiert. Diese werden kontinuierlich aktualisiert und sind überwacht.	☐ Ja	☐ Nein
Alle internetfähigen IT-Systeme (z.B. E-Mail-Server) sind von ihrem vertrauenswürdigen Netzwerk getrennt.	☐ Ja	☐ Nein
Das Netzwerk ist nach Geschäftsfunktionen segmentiert (z.B. ist Datenverkehr zwischen verschiedenen Geschäftsfunktionen blockiert, außer es ist für bestimmte Anforderung notwendig).	☐ Ja	☐ Nein
Das Netzwerk ist nach geografischen Aspekten segmentiert (z.B. ist Datenverkehr zwischen Büros und verschiedenen Standorten blockiert, außer es ist für bestimmte Anforderung notwendig).	☐ Ja	☐ Nein
Es wird eine kontinuierliche Schwachstellenanalyse (Vulnerability Assessment) durchgeführt und sofern notwendig, werden entsprechende Maßnahmen eingeleitet.	☐ Ja	☐ Nein
Es existiert ein Incident- und Change-Management.	☐ Ja	☐ Nein
Der RDP-Port und SMB-Port wurde deaktiviert.	☐ Ja	☐ Nein
Eine EDR-Lösung (End Point Detection & Response) ist auf allen Endpunkten/Servern/ Clientsaktiviert.	☐ Ja	☐ Nein
Eine XDR-Lösung (Extended Detection & Response) ist auf allen kritischen Endpunkten/Servern/ Clients implementiert.	☐ Ja	☐ Nein
Der Datenverkehr zwischen internem und externem Netzwerk sowie dem Internet wird überwacht inkl. Anomalien im Netzwerk sowie Datentransfers.	☐ Ja	☐ Nein
Es gibt dokumentierte Prozesse wie neue Unternehmen in die IT-Infrastruktur und Sicherheitsrichtlinien integriert werden. Netzwerke/Systeme/Anwendungen werden erst nach Erreichen eines vergleichbaren Sicherheitsniveaus integriert.	☐ Ja	☐ Nein
Ihre Kommentare:		

Multifaktor-Authentifizierung (MFA)

Die Multifaktor-Authentifizierung (MFA) ist für folgende Bereiche unternehmensweit verpflichtend implementiert:		
• Fernzugriff auf das Firmennetzwerk inkl. VPN.	☐ 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.	☐ Ja	☐ Nein
Ihre Kommentare:		

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

• Rechenzentren	☐ Ja	☐ Nein	Alert Monitoring	☐ Ja	☐ Nein
• Managed Security	☐ Ja	☐ Nein	Backup and storage	☐ Ja	☐ Nein
• Datenverarbeitung-/Datenspeicherung	☐ Ja	☐ Nein	Cloud Services	☐ Ja	☐ Nein
• Anwendungsmanagement	☐ Ja	☐ Nein	Andere/weitere:	_____	

Es existiert eine schriftliche Outsourcing-Vereinbarung inkl. Sicherheitsanforderungen, die von diesem Dienstleister einzuhalten ist.	☐ Ja	☐ Nein
Es bestehen keine Freistellungs- und/oder haftungsbegrenzende Vereinbarungen mit den externen Dienstleistern.	☐ Ja	☐ Nein
Bitte kommentieren Sie Ihre NEIN-Antworten:		

Cyber-Krisenmanagement

Es existiert ein Krisenreaktionsplan mit folgenden Regelungen:		
• Die Kontaktdaten der Cyber-Krisenhotline von Berkley Deutschland und das Vorgehen zur Schadenmeldung werden in den Krisenreaktionsplan übernommen.	☐ Ja	☐ Nein
• Es existiert ein physischer Business Continuity Plan (BCP).	☐ Ja	☐ Nein
• Es existiert eine physischer Notfall-/Disaster Recovery Plan (DRP).	☐ Ja	☐ Nein
• Der Krisenreaktionsplan, BCP und/oder der DRP wird regelmäßig (mind. jährlich) getestet und aktualisiert.	☐ Ja	☐ Nein
• Es ist sichergestellt, dass auf Vorfälle, auch an Wochenenden oder nachts (Helpdesk/CERT Verfügbarkeit für Vorfälle 24/7), zeitnah reagiert werden kann.	☐ Ja	☐ Nein
Ihre Kommentare:		

Operations Technology (OT)

Wird OT verwendet? (sofern keine OT verwendet wird, ist die Beantwortung der folgenden Fragen nicht notwendig)	☐ Ja	☐ Nein
Wie schnell führt eine Nichtverfügbarkeit Ihrer Systeme zu signifikanten Auswirkungen auf Ihre Geschäftstätigkeit?		
Sofort ☐ nach 6h ☐ nach 12 h ☐ nach 24h ☐ nach 48h ☐		
• Die fortlaufende Produktion/Logistik ist bei Ausfall der IT-Systeme vollständig manuell und offline möglich.	☐ Ja	☐ Nein
• Falls ja: Über welchen Zeitraum, bevor der Geschäftsbetrieb zu einem kompletten Stillstand 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 Produktionsausfall 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 Auslieferungsstillstand kommt?		
Folgende Schutzmaßnahmen sind durchgehend implementiert:		
• Fernzugriffe sind nicht möglich.	☐ 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
• Schnittstellen an Terminals sind deaktiviert.	☐ Ja	☐ Nein
• OT befindet sich in einem separierten Netzwerk.	☐ Ja	☐ Nein
• Zugriffsrechte bestehen ausschließlich für die berechtigten User, die diese zwingend benötigen..	☐ Ja	☐ Nein

• Externe Wartungszugänge sind besonders gesichert (Freigabe, zeitbasiert etc.).	☐ Ja	☐ Nein
• Produktionssysteme werden nach Herstellervorgaben gepatched.	☐ Ja	☐ Nein
• Malwareschutz wird eingesetzt wo möglich.	☐ Ja	☐ Nein
• Es sind Workarounds für nicht patchbare/nicht unterstützte Systeme, z.B. durch restriktives Application-Whitelisting für Produktions-IT (z. B. Supervisory Control and Data Acquisition (SCADA) oder Human Machine Interface (HMI)) implementiert.	☐ Ja	☐ Nein
• Produktionssysteme und -anwendungen sind vollwertig in die Backupstrategie integriert.	☐ Ja	☐ Nein
• Es existiert eine Umgangsrichtlinie mit Lieferanten von Drittsystemen innerhalb Ihrer Produktions-IT.	☐ Ja	☐ Nein
Ihre Kommentare:		

Remote/außerhalb des Büros arbeiten

Es wird sichergestellt, dass die IT-Sicherheitsmaßnahmen und Datenschutzregelungen auch remote eingehalten werden.	☐ 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
Sofern „bring your own device" (BYOD) Geräte verwendet werden:	☐ Ja	☐ Nein
• BYOD Geräte sind in das MDM eingebunden.	☐ Ja	☐ Nein
• Verlust der BYOD Geräte muss gemeldet werden.	☐ Ja	☐ Nein
• Fernlöschung der Unternehmensdaten ist möglich.	☐ Ja	☐ Nein
Ihre Kommentare:		

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

Werden End-of-life (EoL), end-of-Service (EoS) oder Legacy Systeme verwendet?	☐ Ja	☐ Nein
• Es erfolgt eine kontinuierliche Bestandsaufnahme und Bewertung nach Kritikalität von EOL/EOS-Assets sowie Ableitung und Umsetzung von Sicherheitsmaßnahmen.	☐ 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
Ihre Kommentare:		

Elektronischer Zahlungsverkehr (Payment Card Industry)

Speichert, verarbeitet oder übermittelt Ihr Unternehmen/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
Ihre Kommentare:		

IT-Roadmap/ Pläne für das nächste Geschäftsjahr (bitte kurze Beschreibung/Auflistung)

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 potenziellen Umstände/Schäden inklusive Beschreibung auf (insbesondere Datum; Beschreibung der Umstände; Beschreibung der getroffenen Gegenmaßnahmen; Finanzieller Aufwand/Schaden):

Hinweis

Der Unterzeichner erklärt, die obenstehenden Fragen vollständig und wahrheitsgemäß beantwortet zu haben, keine für diese Übernahme/ Fortführung dieser Versicherung wichtigen Aspekte verschwiegen oder nicht richtig wiedergegeben zu haben und verpflichtet sich, Änderungen, die sich vor oder nach dem Abschluss des Vertrages ergeben, unverzüglich und ohne Aufforderung dem Versicherer mitzuteilen (vgl. §§ 19 ff VVG).
Diese ausgefüllte Erklärung und die eventuellen Anlagen werden Bestandteil des Versicherungsvertrages. Mit Unterschrift(en) wird bestätigt, dass vorstehende Angaben vollständig und richtig sind. Der Versicherer ist berechtigt, im Schadenfall sämtliche Angaben zu überprüfen und bei Falschangaben den Versicherungsschutz zu versagen. Die von uns im Fragebogen abgefragten Risikoinformationen sind für uns wesentlich für die Risikobewertung und Vertragsabschluss des Versicherungsvertrages. Auf die Rechtsfolgen der Verletzung der gesetzlichen Anzeigepflicht (Seite 8) wird hingewiesen.

Datenschutz

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: https://www.berkleyeurope.com/datenschutz#deutschland

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 Anzeige-pflichtverletzung 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 Anzeige-pflicht 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 Versicherungs-nehmer 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 Anzeige-pflicht, 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 Um-stände 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 Leistungs-pflicht 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 Versicherungs-nehmer 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.