Drucken Zurücksetzen

Berkley Cyber Risk Protect

Risikoerfassung für mittelständische Unternehmen (Österreich) 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 b) bei der Übertragung (intern und extern)	 ☐ Ja ☐ Ja	 ☐ Nein ☐ 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
Bitte kommentieren Sie Ihre NEIN-Antworten:		

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
Bitte kommentieren Sie Ihre NEIN-Antworten:		

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
Bitte kommentieren Sie Ihre NEIN-Antworten:		

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.	☐ Ja	☐ Nein
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
Bitte kommentieren Sie Ihre NEIN-Antworten:		

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/ Clients aktiviert.	☐ 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
Bitte kommentieren Sie Ihre NEIN-Antworten:		

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
Bitte kommentieren Sie Ihre NEIN-Antworten:		

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 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
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
Bitte kommentieren Sie Ihre NEIN-Antworten:		

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
Bitte kommentieren Sie Ihre NEIN-Antworten:		

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
Mitarbeitende nutzen ausschließlich Firmengeräte.	☐ 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
Bitte kommentieren Sie Ihre NEIN-Antworten:		

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
Bitte kommentieren Sie Ihre NEIN-Antworten:		

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
Bitte kommentieren Sie Ihre NEIN-Antworten:		

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 10) 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 gesetzlichen Anzeigepflicht nach §§ 16 ff VersVG Anzeigepflicht

Die Grundlage unseres Angebotes sind die von Ihnen gemachten Angaben. Daher ist es zwingend notwendig, dass Sie die von uns gestellten Fragen vollständig und wahrheitsgemäß beantworten. Deshalb ist es notwendig, dass Sie auch Umstände angeben, denen Sie nur eine geringe Bedeutung beimessen.

Wir möchten Sie daher darauf hinweisen, dass Sie Ihren Versicherungsschutz gefährden, wenn Sie unrichtige oder unvollständige Angaben machen. Nähre Informationen zu den Folgen einer Verletzung der Anzeigepflicht entnehmen Sie bitte den folgenden Informationen.

Welche vorvertraglichen Anzeigepflichten bestehen?

Beim Abschluss des Versicherungsvertrages sind Sie verpflichtet, alle Ihnen bekannten gefahrerheblichen Umstände, nach denen wir in schriftlicher Form gefragt haben, vollständig und wahrheitsgemäß anzeigen. Sofern wir nach Ihrer Vertragserklärung, aber vor Vertragsannahme in schriftlicher Form nach gefahrerheblichen Umständen fragen, sind Sie auch hier zur Anzeige verpflichtet.

Mögliche Folgen einer vorvertraglichen Anzeigepflicht:

1. Rücktritt und Wegfall des Versicherungsschutzes Verletzen Sie bei Abschluss des Vertrages Ihre Anzeigepflicht, können wir von dem Vertrag zurücktreten. Dies gilt jedoch nicht, wenn Sie nachweisen, dass weder grobe Fahrlässigkeit noch Vorsatz vorliegt.

Bei grob fahrlässiger Verletzung der Anzeigepflicht haben wir kein Rücktrittsrecht, wenn wir den Vertrag auch bei Kenntnis der nicht angezeigten Umstände, wenn auch zu anderen Bedingungen, gezeichnet hätten.

Im Falle des Rücktritts besteht kein Versicherungsschutz. Erklären wir den Rücktritt nach Eintritt des Versicherungsfalles, bleiben wir zur Leistung verpflichtet, wenn Sie nachweisen, dass der nicht oder nicht richtig angegebene Umstand:

- Weder für den Eintritt oder die Feststellung des Versicherungsfalles
- noch für die Feststellung oder den Umfang unserer Leistungspflicht

ursächlich war. Unsere Leistungspflicht entfällt jedoch, wenn Sie die Anzeigepflicht arglistig verletzt haben.

Bei einem Rücktritt steht uns der Teil des Betrages zu, welcher der bis zum Wirksamwerden der Rücktrittserklärung abgelaufenen Vertragszeit entspricht.

2. Vertragsanpassung

Ist unser Rücktrittsrecht ausgeschlossen, da die Verletzung der vorvertraglichen Anzeigepflicht ohne Verschulden erfolgt ist, können wir ab Beginn der laufenden Versicherungsperiode eine höhere Prämie verlangen, falls diese mit Rücksicht auf die höhere Gefahr angemessen ist. Wenn wir den Vertrag unverändert lassen, weil die höhere Gefahr nach unseren Underwriting und tariflichen Grundsätzen auch nicht gegen eine höhere Prämie versicherbar ist, können wir den Vertrag unter Einhaltung einer Frist von einem Monat kündigen.

3. Ausübung unserer Rechte

Wir können unsere Rechte zum Rücktritt, oder zur Vertragsanpassung/ Kündigung nur innerhalb eines Monats schriftlich geltend machen. Die Frist beginnt mit dem Zeitpunkt, zu dem wir von der Verletzung der Anzeigepflicht, die das von uns geltend gemachte Recht begründet, Kenntnis erlangen. Bei der Ausübung unserer Rechte haben wir die Umstände anzugeben, auf welche wir unsere Erklärung berufen. Zur Begründung können wir nachträglich weitere Umstände angeben, wenn für diese die Frist nach Satz 1 nicht verstrichen ist.

Wir können uns auf die Rechte zum Rücktritt oder zur Vertragsanpassung/ Kündigung nicht berufen, wenn wir den nicht angezeigten Gefahrumstand oder die Unrichtigkeit der Anzeige kannten.

Unsere Rechte zum Rücktritt und zur Vertragsanpassung/ Kündigung erlöschen mit Ablauf von drei Jahren nach Vertragsabschluss. Dies gilt nicht für Versicherungsfälle, die vor Ablauf dieser Frist eingetreten sind. Die Frist beträgt zehn Jahre, wenn Sie die Anzeigepflicht arglistig verletzt haben.

4. Stellvertretung durch eine andere Person

Lassen Sie sich durch eine andere Person beim Vertragsabschluss vertreten, so sind bezüglich der Anzeigepflicht, der Vertragsanpassung, des Rücktritts, der Kündigung und der Ausschlussfrist für die Ausübung unserer Rechte die Kenntnis und Arglist Ihres Stellvertreters als auch Ihre eigene Kenntnis und Arglist zu berücksichtigen. Sie können sich nur darauf berufen, dass die Anzeigepflicht nicht vorsätzlich bzw. grob fahrlässig verletzt worden ist, wenn Ihrem Stellvertreter noch Ihnen Vorsatz oder grobe Fahrlässigkeit zur Last fällt.