Berkley Cyber Risk Protect Deutschland

Antragsformular zum Abschluss einer Cyber-Versicherung in Kooperation mit Q Versicherungsmakler GmbH

Berkley DEUTSCHLAND | a Berkley Company

Cyber-Versicherung für Unternehmen bis zu 25 Millionen Euro Umsatz

Antragsformular zum Abschluss einer Cyber-Versicherung

- Informationen zum Deckungsumfang und Highlights
- Antrag zum Abschluss der Cyber-Versicherung
- Mitteilung über die Folgen einer Verletzung der vorvertraglichen Anzeigepflicht
- Gesetzlich vorgeschriebene Informationen
- Berkley Deutschland Cyber-Krisenmanagement
- Informationen zur Echtzeit Cyber-Risikoanalyse und Cyber-Partnerschaften
- Informationsblatt zu Versicherungsprodukten
- Allgemeine Kundeninformationen
- Versicherungsbedingungen

Berkley Cyber Risk Protect – Deckungsumfang & Highlights

Hinweis: Dieses Dokument dient lediglich zu allgemeinen Informationszwecken und begründet keinerlei Ansprüche oder Rechte. Den vollständigen Versicherungsumfang entnehmen Sie bitte den Versicherungsbedingungen und Ihrem Versicherungsschein.

Mit der Berkley Cyber Risk Protect genießen Sie Versicherungsschutz für Drittschäden und Eigenschäden, die sich aus einem Cyber-Vorfall ergeben sowie Assistance-Leistungen im Bereich Cyber-Krisenmanagement. Unser besonderes Angebot: stellen Sie Ihren Cyber-Versicherungsschutz individuell zusammen, sodass dieser optimal Ihren Bedürfnissen entspricht.

Davon profitieren Sie!

✓ **Erfüllung berechtigter sowie Abwehr unbegründeter Haftpflichtansprüche**
Wir befriedigen berechtigte Haftpflichtansprüche und bieten Abwehr bei unberechtigter Ansprüche Dritter.

✓ **Keine „Stand der Technik" Klausel oder versteckte Obliegenheiten**
Wir verzichten auf eine „Stand der Technik Klausel" und haben abschließend geregelte Obliegenheiten.

✓ **Räumlicher Geltungsbereich**
Genießen Sie weltweiten Versicherungsschutz inkl. USA und Kanada, soweit dies rechtlich zulässig ist.

✓ **Kündigungsverzicht im Schadenfall**
Bei einem Versicherungsfall verzichten wir auf unser Kündigungsrecht.

✓ **24/7/365 Cyber-Incident-Response-Hotline inkl. Cyber-Krisenmanagement**
Sie haben einen Cyber-Verdachtsfall? In dieser Situation bieten wir Ihnen eine kostenlose 24/7/365 Cyber-Krisen-Hotline in zahlreichen Landessprachen. Wir bieten Ihnen einen erfahrenen Cyber-Krisenmanager, der Sie kompetent durch die Cyber-Krise begleitet. Dieser Service kann bereits bei einem begründeten Cyber-Verdachtsfall genutzt werden.

✓ **Kein Selbstbehalt für das Cyber-Krisenmanagement und Rückforderungsverzicht**
Für das Cyber-Krisenmanagement besteht kein Selbstbehalt innerhalb der vereinbarten Zeitspanne! Wir verzichten auf unser Rückforderungsrecht, sollte sich später herausstellen, dass trotz begründetem Verdacht kein versichertes Schadenereignis vorlag.

✓ **Weltweites und unabhängiges Expertennetzwerk in der Cyber-Krise**
Bei der Cyber-Krisenbewältigung unterstützt Sie unser weltweites Expertennetzwerk schnell und professionell. Dazu zählen IT-Forensiker, PR-Agenturen, Call-Center und Datenschutzanwälte. Die Koordinierung und Unterstützung erfolgt durch unseren Cyber-Krisenmanager.

✓ **(Datenschutz-) Verfahren inkl. interner Untersuchungen und freiwillige Selbstanzeige**
Wir bieten einen weitgehenden Versicherungsschutz bei behördlichen Ermittlungen und Verfahren inklusive der Kostenübernahme für interne Untersuchungen.

✓ **Absicherung von zielgerichteten und nicht-zielgerichteten Cyber-Angriffen**
Versicherungsschutz ist für Sie bei zielgerichteten und nicht-zielgerichteten Cyber-Angriffen, wie beispielsweise der Übermittlung von Schadprogrammen, garantiert!

✓ **Vorrangiger Versicherungsschutz unserer Cyber-Versicherung**
Für Cyber-Versicherungsfälle geht unsere Cyber-Versicherung als Spezialversicherung vor und Sie können sofort auf unser Cyber-Krisenmanagement zurückgreifen.

✓ **Zeitlicher Geltungsbereich**
Wir bieten eine unbegrenzte Rückwärtsversicherung für unbekannte und schadenauslösende Ereignisse vor Versicherungsbeginn sowie eine automatische Nachmeldefrist.

✓ **Verdachtsfall und Beweislasterleichterung**
Grundsätzlich liegt die Beweislast bei der Versicherungsnehmerin, die Anforderungen hierfür haben wir durch die Beweislasterleichterung deutlich reduziert. Zusätzlich wird der Versicherungsschutz bei uns bereits bei einem begründeten Verdachtsfall ausgelöst.

✓ **Goodwill-Aktionen**
Wir bieten neben der Kostenerstattung für die Vorbereitungsmaßnahmen auch die Möglichkeit der Kostenübernahme für die tatsächliche Einlösung von Goodwill-Aktionen.

✓ **Enger Repräsentanten-Begriff**
Wir stellen bei Repräsentanten ausschließlich auf die der Versicherungsnehmerin ab.

✓ **Pauschale Konzerndeckung sowie automatische Vorsorgedeckung**
Für eine Vielzahl von neu hinzukommenden Tochtergesellschaften bieten wir automatischen Versicherungsschutz. Bei allen anderen gewähren wir eine automatische und prämienneutrale Vorsorgedeckung.

✓ **Cyber-Kriminalität**
Wir bieten u.a. Versicherungsschutz für erhöhte Telekommunikationskosten, unautorisierte Überweisungen und unautorisierte Warenlieferungen durch den unberechtigten Zugang Dritter zum IT-System von Versicherten.

✓ **Absicherung von physischen und digitalen Daten**
Bei uns sind Ihre digitalen und physischen Daten im Versicherungsschutz berücksichtigt.

✓ **Bedienfehler**
Automatischen Versicherungsschutzen gewähren wir infolge von Bedienfehlern.

✓ **Kostenübernahme für Informationspflichten gemäß DSGVO, BDSG und vergleichbaren ausländischen Rechtsnormen**
Es sind Benachrichtigungskosten für Kunden, Betroffene und Behören entstanden? Wir übernehmen diese – auch ohne gesetzliche Verpflichtung.

✓ **Kosten für Monitoring-Dienstleistungen**
Anfallende Kosten für Monitoring-Dienstleistungen bei Kreditkarten-/Identitätsdiebstahl werden von uns getragen.

✓ **Ausfall externer IT-Dienstleistungen**
Wir bieten automatischen Versicherungsschutz für den Ausfall externer IT-Dienstleistungen, wenn diese aufgrund einer Informationssicherheitsverletzung Ihnen nicht zur Verfügung stehen.

✓ **Rechteverletzung durch digitale Medien**
Wir bieten Versicherungsschutz für die Freistellung berechtigter und die Abwehr unberechtigter Schadenersatzansprüche Dritter, aufgrund von Urheberrechts-, Markenrechts-, oder Persönlichkeitsrechtsverletzungen.

✓ **Cyber-Betriebsunterbrechung**
Cyber-Krisensituationen sind oftmals mit kostspieligen Betriebsunterbrechungen verbunden. Wir ersetzen den entgangenen Betriebsgewinn und die fortlaufenden Kosten (Cyber-Ertragsausfallschaden). Außerdem übernehmen wir die Mehrkosten zur Wiederherstellung des Geschäftsbetriebes. Es findet ausschließlich der zeitliche Selbstbehalt Anwendung.

✓ **Schadenminderungskosten**
Wir ersetzen auch die angemessenen und notwendigen erfolglos aufgewendeten Schadenminderungskosten.

✓ **Versicherungsschutz für Finanzdienstleister**
Sie sind ein Unternehmen der Finanzdienstleistungsbranche? Gerne bieten wir auch Ihnen unseren umfassenden Versicherungsschutz.

✓ **Optionale Bausteine**
Gerne prüfen wir auch den Einschluss unserer optionalen Deckungsbausteine sowie individuelle Sondervereinbarungen.

✓ **Vereinfachter Antrag**
Für Unternehmen mit einem konsolidierten Jahresumsatz von maximal 25 Millionen Euro bieten wir einen vereinfachten Antragsprozess zum Abschluss der Versicherung.

✓ **Echtzeitbewertung der von außen sichtbaren IT-Infrastruktur**
Sie wollen wissen, wie Ihr Unternehmen über online öffentlich zugängliche Systeme einsehbar ist? Bei Vertragsbeginn und Vertragsverlängerung liefern wir Ihnen einen Bericht über die Echtzeitbewertung Ihrer IT-Infrastruktur. Wir geben Ihnen hiermit eine Detailübersicht über Ihre IT-Infrastruktur und potenzielle Schwachstellen sowie Handlungsempfehlungen. Für unsere Cyber-Kunden ist dieser Service kostenlos!

Drucken Zurücksetzen

Antrag auf Abschluss einer Berkley Cyber Risk Protect – Deutschland
Versicherung für Unternehmen mit Jahresumsatz bis maximal 25 Millionen Euro

1. Angabe zum Versicherungsmakler in Kooperation mit Q Versicherungsmakler GmbH

Versicherungsmakler:	E-Mail-Adresse:

Über Q Versicherungsmakler GmbH

Q Versicherungsmakler GmbH ist ein unabhängiger Versicherungsmakler. Q Versicherungsmakler GmbH hat sich auf die Absicherung bestimmter Berufsgruppen spezialisiert und bietet leistungsstarke Versicherungsprodukte, welche auf die Bedürfnisse der jeweiligen Berufsgruppen bestmöglich zugeschnitten sind. Q Versicherungsmakler GmbH bietet seinen Kunden persönlichen Service durch kompetente Berater und unterstützt seine Kunden mit effizienten Online-Prozessen. Als Branchenspezialist stellt Q Versicherungsmakler GmbH Produkte und Services auch anderen Versicherungsmaklern und Onlineplattformen zur Verfügung.

2. Stammdaten zur Versicherungsnehmerin in Deutschland

Firmierung:			
Straße:		Postleitzahl:	Ort:
Gründungsdatum:	Tätigkeit/Branche:		Homepage:

3. Versicherungsbeginn

Versicherungsbeginn (Tag/Monat/Jahr):
Abweichende Hauptfälligkeit (Tag/Monat):
Die Mindesversicherungsperiode ist 9 Monate und maximal 18 Monate.

Hinweis:
Der Versicherungsbeginn kann maximal 4 Monate in der Zukunft liegen. Der Versicherungsschutz gilt frei von bekannten Schäden, Umständen und Pflichtverletzungen zum Vertragsbeginn.

4. Risikofragen zur Versicherungsnehmerin inkl. Tochtergesellschaften

1. Die Versicherungsnehmerin ist seit mehr als 12 Monaten operativ tätig, hat Ihren Hauptsitz in Deutschland und es besteht derzeit keine Berkley Cyber Risk Protect Versicherung.	Ja
2. Der Tätigkeitsbereich umfasst **nicht** die folgenden Bereiche: • Finanzdienstleister (Zahlungsabwicklung, Kredit Rating Agentur, Inkassodienstleistungen, Vermittlung/ Beratung zu Bank- Versicherungsprodukten, Vermögensverwaltung, Versicherungsmakler, etc.) • Glücksspiel, Pornografie, Datensammlung und -speicherung • Stadtwerke, Behörden, Städte, Gemeinden und sonstige staatliche/ öffentliche Einrichtungen inkl. öffentliche Versorgungsunternehmen, Fluggesellschaften und Flughäfen • Handelsplattformen und Dating-Plattformen • IT-Unternehmen und Telekommunikationsunternehmen (Cloud-Service-Provider, Rechenzentrum, Software-/App-/ Hardwarehersteller, Internet Service Provider, Telekommunikationsanbieter, etc.) • Call-Center, Direktmarketing, Franchisenehmer, Franchisegeber und Betreiber von Online-Shops, Internetplattformen und sozialen Netzwerken, Gemeinnützige Organisationen, politische Parteien und Religionsgemeinschaften • Gastgewerbe: Hotels, Hostels, Restaurants, Bars, etc. • Gesundheitswesen (Ärzte, Krankenhäuser, Pflegeheime, Heilberufe, Covid-19 Teststationen, etc.)	Ja
3. Es werden maximal 25% des jährlichen Gesamtumsatzes in den USA/ Kanada erwirtschaftet (Tochtergesellschaften/ Niederlassungen müssen separat angefragt werden).	Ja

4.	Es Bezahlen jährlich keine oder höchstens bis zu 50.000 Kunden bei Ihnen mit Kreditkarte. Wenn Sie Kreditkartenzahlungen akzeptieren, erfüllen Sie bzw. Ihr Zahlungsdienstleister die PCI DSS (Payment Card Industry Data Security Standard).	Ja
5.	Es gibt eine unternehmensweite schriftliche Passwort-Policy inkl. Vorgaben zur Komplexität und zeitlichen Gültigkeit (max. 90 Tage) bzw. dies wird technisch erzwungen.	Ja
6.	Es gibt unternehmensweit regelmäßige (mindestens jährliche) Mitarbeiterschulungen zum Thema Informationssicherheit sowie Informationen über aktuelle Gefahrenpotenziale (z.B. Newsletter über aktuelle Trojaner, Phishing).	Ja
7.	Die Kontaktdaten der Cyber-Krisenhotline von Berkley Deutschland und das Vorgehen zur Schadenmeldung/ Cyber-Krisenmanagement werden in den Krisenreaktionsplan übernommen.	Ja
8.	Unternehmensweit gelten mindestens die folgenden IT-Schutzmaßnahmen: • Virenschutz mit automatischer Update-Funktion auf Servern und Clients (Desktop-Computer, Laptops und Terminals). • Firewallstrukturen an allen Netzübergängen zum Internet. • Abgestuftes Rechtekonzept mit administrativen Kennungen ausschließlich für IT-Verantwortliche. • Tägliche Backups (bis 1 Millionen Euro Umsatz mindestens wöchentlich) sowie ständiges Vorhandensein von mindestens einer vollständigen Offline-Datensicherung, die jeweils nicht älter als eine Woche ist. • Sie spielen regelmäßig und zeitnah (innerhalb von 30 Tagen) Sicherheitsupdates und Patches nach Herstellervorgaben ein. • Es wurde die Relevanz von lokal anwendbaren Datenschutzbestimmungen (insbesondere DSGVO) abgeklärt und gegebenenfalls Maßnahmen abgeleitet.	Ja
9.	Bei sogenannten „bring your own device“ Geräten, bei „work from home“ bzw. „remote Arbeiten“ gilt folgendes: • Multi-Faktor Authentifizierung für Fernzugriffe auf das Firmennetzwerk • Die Verbindung zum Firmennetzwerk erfolgt ausschließlich über abgesicherte Zugangsmöglichkeiten (VPN, Citrix, VDI, etc.). • Es wird eine aktuelle Software/ Betriebssystem verwendet, E-Mails werden verschlüsselt gespeichert und es gibt ein Verzeichnis über BYOD-Geräte im Unternehmen (sofern erlaubt); Der Benutzer muss einen Verlust des Gerätes unverzüglich dem Unternehmen anzeigen und eine Fernlöschung der Firmendaten ist möglich. • Es gibt keine Einschränkungen bei Malware-/ Virenerkennung, Patchmanagement und Backups.	Ja
10.	Cyber-Kriminalität: • Sie haben Sie ein verpflichtendes 4-Augen-Prinzip bei Überweisungen über 10.000 Euro sowie MFA für die Online-Überweisungsfreigabe. • Bei Telefonanlagen, Anrufbeantworter, Smartphones, PC etc. haben Sie die Passwörter und PIN von der Werkseinstellung geändert. • Es wurden geeignete Maßnahmen getroffen, um unautorisierte Warelieferungen zu vermeiden.	Ja
11.	Es bestehen keine Haftungsfreistellungen mit den externen IT-Dienstleistern (MS Office 360 ist ausgenommen) und Minimum Sicherheitsstandards werden beim IT-Dienstleister eingehalten.	Ja
12.	Es sind Ihnen aus den letzten drei Jahren keine Umstände oder Schäden bekannt die zu einem Versicherungsfall unter dieser Cyber-Versicherung fallen würden? *Dies beinhaltet u.a. Hacker-Angriffe, interne/ externe Ermittlungen und Untersuchungen in Bezug auf Datenschutzverletzungen, Vorfälle durch Schadprogramme, Cyber-Erpressungen, Bedienfehler, Datenverlusten, technische Probleme, ungeplante Betriebsunterbrechungen sowie Schadenersatzansprüche von Dritten in Bezug auf Datenrechtsverletzungen oder drohenden/ anhängigen Verfahren von Datenschutzbehörden.*	Ja

Bitte kurze Auflistung sowie explizite Nennung des drei unternehmenskritischen Dienstleisters im Bereich Cloud/ SaaS, PaaS, etc:

Externer IT-Dienstleister	Tätigkeit

Hinweis:

Wenn Sie eine oder mehrere der nachfolgenden Risikofragen nicht mit „Ja" beantworten können, höhere als die aufgeführten Versicherungssummen bzw. Umsätze oder weitere Risikoorte versichern wollen, schicken Sie uns bitte den ausgefüllten Berkley Cyber Risk Protect Fragebogen für ein individuelles Angebot an cyber@qversicherung.de.

5. Berechnung der Jahresnettoprämie

Versicherungssumme in Euro	Konsolidierter Gesamtumsatz in Euro bis einschließlich						
	100.000 €	**150.000 €**	**200.000 €**	**250.000 €**	**500.000 €**	**750.000 €**	**1.000.000 €**
250.000 €	450 Euro	480 Euro	500 Euro	520 Euro	575 Euro	630 Euro	675 Euro
500.000 €	550 Euro	600 Euro	640 Euro	665 Euro	700 Euro	780 Euro	840 Euro
1.000.000 €	700 Euro	750 Euro	800 Euro	850 Euro	940 Euro	950 Euro	1.050 Euro

Versicherungssumme in Euro	Konsolidierter Gesamtumsatz in Euro bis einschließlich					
	1.500.000 €	**2.000.000 €**	**2.500.000 €**	**3.000.000 €**	**4.000.000 €**	**5.000.000 €**
250.000 €	720 Euro	775 Euro	830 Euro	875 Euro	910 Euro	950 Euro
500.000 €	930 Euro	1.000 Euro	1.040 Euro	1.100 Euro	1.150 Euro	1.220 Euro
1.000.000 €	1.200 Euro	1.230 Euro	1.350 Euro	1.390 Euro	1.500 Euro	1.620 Euro
1.500.000 €	1.250 Euro	1.450 Euro	1.540 Euro	1.600 Euro	1.640 Euro	1.730 Euro
2.000.000 €	./.	1.750 Euro	1.900 Euro	1.920 Euro	2.130 Euro	2.230 Euro

Versicherungssumme in Euro	Konsolidierter Gesamtumsatz in Euro bis einschließlich				
	7.500.000 €	**10.000.000 €**	**15.000.000 €**	**20.000.000 €**	**25.000.000 €**
500.000 €	1.420 Euro	1.650 Euro	2.100 Euro	2.500 Euro	2.950 Euro
1.000.000 €	1.900 Euro	2.200 Euro	2.500 Euro	2.600 Euro	3.450 Euro
1.500.000 €	2.000 Euro	2.350 Euro	2.950 Euro	3.350 Euro	3.700 Euro
2.000.000 €	2.200 Euro	3.050 Euro	3.250 Euro	3.450 Euro	5.000 Euro

Hinweis:

Die Versicherungsprämien sind Jahresnettoprämien (zuzüglich der aktuell geltenden Versicherungssteuer i.H.v. 19%).

Höhere Versicherungssummen oder höhere Umsätze werden auf individueller Basis quotiert. Für diese Angebotserstellung bitten wir um Zusendung des ausgefüllten Berkley Cyber Risk Protect Fragebogen.

6. Besondere Bedingungen

- Berkley Deutschland Cyber-Krisenmanagement (vgl. Seite 15)
- Es besteht kein Versicherungsschutz aufgrund von oder im Zusammenhang mit dem Kaseya VSA Supply-Chain Ransomware-Angriff (CVE-2021-30116).
- Es besteht kein Versicherungsschutz aufgrund von oder im Zusammenhang mit den Schwachstellen in Microsoft Exchange (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065).
- Es besteht kein Versicherungsschutz aufgrund von oder im Zusammenhang mit der Schwachstelle in log4j (CVE-2021-44228,CVE-2021-45046, CVE-2021-45105).

Hinweis zur Versicherungssteuer:
Die Versicherungsprämien sind Jahresnettoprämien (zuzüglich der aktuell geltenden Versicherungssteuer i.H.v. 19%).

7. Selbstbehalte

Monetärer Selbstbehalt:	5.000 Euro
Zeitlicher Selbstbehalt im Rahmen der Betriebsunterbrechung	12 Stunden
Cyber-Krisenmanagement gemäß Ziffer V.1., 2. und 4. der Versicherungsbedingungen:	0 Euro für einen Zeitraum von bis zu 72 Stunden nach erstmaliger Feststellung durch Versicherte oder Repräsentanten. Die 72 Stunden Frist beginnt mit der Kontaktaufnahme des vereinbarten Cyber-Krisenberater über die Berkley Deutschland Cyber-Krisenhotline.

Alternative:

Monetärer Selbstbehalt	10.000 Euro	Abschlag Jahresnettoprämie: -10%

Für die Wahl des alternativen Selbstbehaltes i. H. v. 10.000 EUR setzen Sie bitte nachfolgend ein Kreuz: ☐

8. Haftzeit im Rahmen der Betriebsunterbrechung

Es gilt eine Haftzeit von 180 Tagen.

9. Bedingungswerk

Bei Vertragsabschluss werden die Berkley Cyber Risk Protect Bedingungen - Deutschland Stand 05.2022 Version Q Versicherungsmakler GmbH sowie die Besondere Deckungsvereinbarung „Sublimite“ gemäß der vereinbarten Sublimite dieses Antrages sowie die besonderen Bedingungen gemäß Ziffer 6 vereinbart.

10. Versicherungssumme

Die vereinbarte Versicherungssumme ist 1-fach maximiert.

11. Sublimite

Für folgende Deckungsbausteine der Versicherungsbedingungen gelten die nachfolgenden Sublimite vereinbart:

Sachschaden an der Computer Hardware (Ziffer II.2.c)	50.000 Euro
Forensische Buchhaltung (Ziffer II. 3b viii)	50.000 Euro
Technische Probleme (Ziffer II. 3b ix)	250.000 Euro
Ausfall externer IT-Dienstleistungen (ZIffer II. 3bx)	250.000 Euro
Cyber-Erpressung (Ziffer II. 3c)	50% der Versicherungssumme, max. 1 MEUR
Cyber-Kriminalität (Ziffer II. 3d)	250.000 Euro
Interne Untersuchungen und Ermittlungen (Ziffer III. 3c)	50.000 Euro
Consumer Redress Fund (Ziffer: III. 3d)	100.000 Euro
Entschädigungen mit Strafcharakter, Bußgelder, Gebühren (Ziffer: IV)	50% der Versicherungssumme, max. 1 MEUR
Schadenminderung (Ziffer: I.2)	10% der Versicherungssumme, max. 1 MEUR
E-Discovery (Ziffer: VI. 3)	100.000 Euro
Freiwillige Selbstanzeige (Ziffer: VI.5)	50.000 Euro
Cyber-Verdachtsfall und Rückforderungsverzicht (Ziffer: IX.3c)	25.000 Euro

11. Übersicht zum gewählten Versicherungsschutz und Versicherungsprämie

Jahresnettoprämie:	0,00 €
Reduzierung bei alternativem Selbstbehalt:	0,00 €
Jahresnettoprämie Gesamt:	0,00 €
Jahresprämie inkl. Versicherungssteuer für 1 Jahr:	**0,00 €**

13. SEPA-Lastschriftmandat

Ich/ Wir ermächtige(n) Q Versicherungsmakler GmbH, Zahlungen von meinem/unserem Konto mittels Lastschrift einzuziehen. Zugleich weise(n) ich/wir mein/unser Kreditinstitut an, die von Q Versicherungsmakler GmbH auf mein/unser Konto bezogenen Lastschriften einzulösen.

Hinweis: Dieses Lastschriftmandat dient nur dem Einzug von Lastschriften, die auf Konten von Unternehmen gezogen sind. Ich bin/Wir sind nicht berechtigt, nach der erfolgten Einlösung eine Erstattung des belasteten Betrages zu verlangen. Ich bin/Wir sind berechtigt, mein/unser Kreditinstitut bis zum Fälligkeitstag anzuweisen, Lastschriften nicht einzulösen.

Gültig ab:	
Name bzw. Firmenstempel (Kontoinhaber):	
Straße und Hausnummer:	
Postleitzahl und Ort:	
Mandatsreferenz:	Wird separat mitgeteilt
Gläubiger-Identifikationsnummer:	DE52ZZZ00001837862
Kreditinstitut (Name):	
IBAN:	
SWIFT-BIC:	

Falls das Konto die erforderliche Deckung nicht aufweist, besteht für das Geldinstitut keine Verpflichtung zur Einlösung. Bearbeitungsgebühren der beteiligten Banken für die Nichteinlösung einer Lastschrift, die von mir zu vertreten sind (z.B. Konto erloschen, keine ausreichende Deckung), gehen zu meinen Lasten.

14. Gültigkeit des Cyber-Antragsmodells

Dieser Cyber-Antrag hat eine Bindungswirkung bis zum 31.12.2022 und ersetzt alle vorherigen Cyber-Anträge. Ab diesem Zeitpunkt ist unser Angebot nicht mehr gültig.

15. Annahmeerklärung

Diese ausgefüllte Annahmeerklärung und die beigefügten Anlagen sind Basis der Versicherung und werden deshalb ein Bestandteil des Versicherungsvertrages. Mit Unterschrift(en) des Repräsentanten der Versicherungsnehmerin i.S.d. Versicherungsbedingungen wird bestätigt, dass vorstehende Angaben vollständig und richtig sind und dass Sie folgende Dokumente rechtzeitig vor Antragsstellung erhalten und zur Kenntnis genommen haben: Versicherungsbedingungen Berkley Cyber Risk Protect 05/2022 Version Q Versicherungsmakler GmbH, Besondere Bedingungen gemäß dieses Antrages, Mitteilung über die Folgen einer Verletzung der vorvertraglichen Anzeigepflicht, Hinweis zur Datenschutzerklärung, gesetzlich vorgeschriebene Informationen, Informationsblatt zu Versicherungsprodukten, Allgemeine Kundeninformationen, Berkley Deutschland Cyber Krisenmanagement, Realtime Cyber-Risikoanalyse und Cyber-Partnerschaften.

Bei den Risikoangaben handelt es sich um vorvertragliche Anzeigen. Bitte beachten Sie hierzu auch die beigefügte Erklärung bei Verletzung der vorvertraglichen Anzeigepflicht.

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

Hinweis:
Eine Unterzeichnung des Antrages, bzw. Beantwortung der Risikofragen durch den Versicherungsvermittler ist nicht möglich. Dies kann ausschließlich durch einen Repräsentanten i.S.d. Versicherungsbedingungen erfolgen.

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.

Gesetzlich vorgeschriebene Informationen

Was gilt, wenn Sie den ersten oder einmaligen Beitrag nicht rechtzeitig zahlen?

Gefährdung des Versicherungsschutzes

Der Beginn des Versicherungsschutzes ist von der rechtzeitigen Zahlung abhängig. Zahlen Sie den ersten oder einmaligen Beitrag nicht rechtzeitig, beginnt der Versicherungsschutz daher erst zu dem Zeitpunkt, zu dem Sie den Beitrag zahlen. Für Versicherungsfälle, die in der Zwischenzeit eintreten, sind wir nicht zu Leistungen verpflichtet.

Unsere Leistungspflicht bleibt bestehen, wenn Sie nachweisen, dass Sie die Nichtzahlung nicht zu vertreten haben.

Unser Rücktrittsrecht

Zahlen Sie den ersten oder einmaligen Beitrag nicht rechtzeitig, können wir vom Vertrag zurücktreten, solange Sie die Zahlung nicht bewirkt haben. Das Rücktrittsrecht ist ausgeschlossen, wenn Sie nachweisen, dass Sie die Nichtzahlung nicht zu vertreten haben.

Ergänzenden Informationen in Versicherungsschein und Versicherungsbedingungen

Regelungen zum Beginn des Versicherungsschutzes, zur Fälligkeit des ersten oder einmaligen Beitrages und zur Rechtzeitigkeit der Zahlung können Sie dem Versicherungsschein sowie den für Ihren Vertrag geltenden Versicherungsbedingungen entnehmen.

Widerrufsbelehrung

Widerrufsrecht

Sie können Ihre Vertragserklärung innerhalb von 14 Tagen ohne Angabe von Gründen in Textform (z.B. Brief, Fax, E-Mail) widerrufen. Die Frist beginnt, nachdem Sie den Versicherungsschein, die Versicherungsbestimmungen einschließlich der Allgemeinen Versicherungsbedingungen, die weiteren Informationen nach § 7 Abs. 1 und 2 des Versicherungsvertragsgesetzes in Verbindung mit den §§ 1 bis 4 der VVG-Informationspflichtenverordnung und diese Belehrung jeweils in Textform erhalten haben. Zur Wahrung der Widerrufsfrist genügt die rechtzeitige Absendung des Widerrufs.

Der Widerruf ist zu richten an:

W. R. Berkley Europe AG - Niederlassung für Deutschland
Christophstraße 19
50670 Köln
oder
per Fax an +49 (0) 221 37050048 oder per E-Mail an wrbvd_info@wrberkley.com

Widerrufsfolgen

Im Falle eines wirksamen Widerrufs endet Ihr Versicherungsschutz, und wir erstatten Ihnen den auf die Zeit nach Zugang des Widerrufs entfallenden Teil des Beitrages, wenn Sie zugestimmt haben, dass der Versicherungsschutz vor dem Ende der Widerrufsfrist beginnt. Den Teil des Beitrages, der auf die Zeit bis zum Zugang des Widerrufs entfällt, dürfen wir in diesem Fall einbehalten; dabei handelt es sich um einen Betrag in Höhe von 1/360 pro Tag des Jahresbeitrages, an dem Versicherungsschutz bestand. Die Erstattung zurückzuzahlender Beträge erfolgt unverzüglich, spätestens 30 Tage nach Zugang des Widerrufs. Beginnt der Versicherungsschutz nicht vor dem Ende der Widerrufsfrist, hat der wirksame Widerruf zur Folge, dass empfangene Leistungen zurückzugewähren und gezogene Nutzungen (z. B. Zinsen) herauszugeben sind.

Besondere Hinweise

Ihr Widerrufsrecht erlischt, wenn der Vertrag auf Ihren ausdrücklichen Wunsch sowohl von Ihnen als auch von uns vollständig erfüllt ist, bevor Sie Ihr Widerrufsrecht ausgeübt haben.
Ein Widerrufsrecht besteht nicht bei Versicherungsverträgen über ein Großrisiko im Sinne des § 210 VVG, über vorläufige Deckung, mit einer Laufzeit von weniger als einem Monat, bei Pensionskassen, die auf arbeitsvertraglichen Regelungen beruhen.

Ende der Widerrufsbelehrung

Crawford & Company – Dienstleister für das Cyber-Krisenmanagement

In der Cyber-Krise die Kontrolle behalten. Neben optimalen Versicherungslösungen gelingt dies durch ein professionelles und zielstrebiges Cyber-Krisenmanagement. Als Versicherungsnehmerin von Berkley Deutschland bieten wir Ihnen Expertise von Crawford & Company, einer weltweit größten Dienstleister im Bereich Schadenmanagement.

Crawford unterstützt Sie im Falle eines Cyber-Vorfalls/begründeten Verdachtsfalls bei der Bewältigung der Cyber-Krise — vollumfänglich und unabhängig. Mit dem Zugriff auf ein umfangreiches Expertennetzwerk (u.a. aus dem Bereich IT-Forensik, Krisenkommunikation/PR und Datenschutz/-sicherheit) verfügt Crawford über die notwendigen Ressourcen, um Sie in der Cyber-Krise aktiv zu unterstützen. Die externen Netzwerkpartner sind nach einer Due Diligence Prüfung vertraglich mit Crawford verbunden, was Verfügbarkeit, Know-How und die Einhaltung von Service Level Agreements garantiert. Crawford agiert als unabhängiger Cyber-Krisenmanager für die Versicherten von Berkley Deutschland. Für die Durchführung und den Erfolg der Maßnahmen ist Berkley Deutschland nicht verantwortlich und übernimmt keine Haftung. Ansprüche aus der Inanspruchnahme der Dienstleistung sind von der Versicherungsnehmerin direkt gegen den Dienstleister zu stellen.

Bitte beachten Sie, dass sich sowohl die bevorzugten Krisendienstleister, als auch die Netzwerkpartner von Zeit zu Zeit ändern können und das Netzwerk kontinuierlich erweitert wird. Dies ist notwendig, um Ihnen die bestmögliche Unterstützung im Falle eines Cyber-Krisenfalls zu bieten. Unsere derzeit bevorzugten Partnerunternehmen im Bereich Cyber-Krisenmanagement finden Sie unter:

www.berkleyversicherung.de/produkte/cyber/

Bitte beachten Sie, dass nicht alle Krisendienstleister in jedem Land zur Verfügung stehen.

Ihr Kontakt:
Crawford & Company (Deutschland) GmbH
Werdener Straße 4
40227 Düsseldorf

Cyber-Krisenmanagement: Soforthilfe im Cyber-Notfall – die wichtigsten Infos

Hinweis: Dieses Dokument ist Bestandteil Ihrer Cyber-Versicherungspolice

Bitte wenden Sie sich im Cyber-Krisenfall unverzüglich telefonisch an Ihren persönlichen Cyber-Krisenmanager:
Berkley Deutschland Cyber-Krisenhotline:

(die entsprechenden Telefonnummern erhalten Sie bei Vertragsabschluss)

Erreichbarkeit: 24/7/365 in zahlreichen Landessprachen

1. Cyber-Krisenhotline

Melden Sie Ihren Cyber-Vorfall unverzüglich. Nutzen Sie hierzu unsere kostenlose und 24 Stunden erreichbare Cyber-Krisenhotline. Diese ist in zahlreichen Landessprachen verfügbar. Halten Sie bitte bereit:

- Ihre Kontaktdaten
- Ihre Versicherungsscheinnummer
- Details zum Cyber-Vorfall

2. Cyber-Krisenmanager

Ihr persönlicher Cyber-Krisenmanager von Crawford wird Sie umgehend kontaktieren und das weitere Vorgehen besprechen. Dieser wird Experten aus dem weltweiten Netzwerk einschalten Empfehlungen aussprechen, um die Cyber-Krise schnellstmöglich zu beenden. Ihr Vorteil: Sie profitieren von Beginn an von einem erfahrenen Cyber-Krisenmanager.

3. Einschaltung des Expertennetzwerks

Der Cyber-Krisenmanager koordiniert für Sie den Cyber-Vorfall und schaltet in Abstimmung mit Ihnen die notwendigen Experten aus unserem weltweiten Netzwerk ein. Die finale Auswahl der notwendigen Dienstleister von Crawford bleibt Ihre Entscheidung. Sofern Sie andere Dienstleister einschalten möchten, die nicht Teil des Expertennetzwerkes sind, ist dies vorab mit uns zu vereinbaren – im Idealfall bei Vertragsabschluss. Zusätzlich erfolgt durch Crawford eine Abstimmung und Klärung notwendiger/gewünschter Maßnahmen mit dem Versicherer (Klärung der Deckung sowie Klärung der Kostenübernahme).

4. Beauftragung

Die Inanspruchnahme der Dienstleister aus unserem Expertennetzwerk erfolgt durch Ihre Beauftragung und Gegenzeichnung eines entsprechenden Vertrages. Als Kunde der W. R. Berkley Europe AG profitieren Sie von unseren Sonderkonditionen. Für die Schadenregulierung reichen Sie uns die jeweilige Rechnung zur Prüfung ein und wir erstatten Ihnen die versicherten Kosten. W. R. Berkley Europe AG übernimmt keine Haftung aus den Dienstleistungen, die durch Krisendienstleister ausgeführt wurden. Der Versicherer hat keine Rechte und übernimmt daher keine Verpflichtungen aus dem Vertrag, der zwischen der Versicherungsnehmerin und den Krisendienstleistern geschlossen wird. Sämtliche Rechte und Pflichten aus solch einer Vereinbarung, insbesondere Rechnungen, Gebühren und Leistungen gehen zu Nutzen und Lasten der Versicherungsnehmerin. Dies garantiert gleichzeitig eine unabhängige und objektive Bewältigung der Cyber-Krise.

5. Schadenmeldung

Melden Sie unverzüglich W. R. Berkley Europe den Cyber-Vorfall parallel. Der Anruf bei unserer Cyber-Krisenhotline ersetzt die Schadenmeldung nicht.

Sofern explizit gewünscht, übernimmt Ihr persönlicher Cyber-Krisenmanager dies gerne für Sie.

Die Schadenmeldung richten Sie bitte an: wrbvd_schaden_cyber@wrberkley.com

6. Informationsaustausch

Transparent und strukturiert durch die Cyber-Krise. Im Cyber-Krisenmanagement fungiert Ihr persönlicher Cyber-Krisenmanager als zentraler Ansprechpartner, sorgt für einen regelmäßigen Informationsaustausch und koordiniert das Vorgehen zwischen allen Beteiligten. Nach Beendigung des Cyber-Vorfalls erstellt dieser einen Abschlussbericht für W. R. Berkley Europe AG. Regelmäßige Telefonkonferenzen zwischen der Versicherungsnehmerin, den Dienstleistern, dem Cyber-Krisenmanager, Ihrem Versicherungsmakler und dem Versicherer dienen zur Besprechung des Vorgehens bzw. Klärung von Fragen und erleichtert die Schadenregulierung für alle Beteiligten.

FAQ zum Cyber-Krisenmanagement

Welche Dienstleistungen umfasst das Cyber-Krisenmanagement?

Mit dem Abschluss Ihrer Cyber-Versicherung bei W. R. Berkley Europe AG haben Sie Zugriff auf unser Cyber-Krisenmanagement. Dieses beinhaltet eine kostenlose Cyber-Krisenhotline, einen Cyber-Krisenmanager und unabhängige Experten aus den Bereichen IT-Forensik, PR-/Krisenkommunikation und Datenschutzrecht. Dies ist ein essenzieller Bestandteil unserer Cyber-Versicherung. Unsere Experten helfen Ihnen schnell und unkompliziert in der Cyber-Krise und verringern die Folgen einer Cyber-Krise für Sie massiv. Die mit uns und dem Cyber-Krisenmanager abgestimmten Dienstleistungen sind über Ihre Cyber-Versicherung abgedeckt. Alle Informationen zur Art und Umfang der Dienstleistungen können Sie den vereinbarten Versicherungsbedingungen entnehmen.

Wenn ich die Cyber-Krisenhotline für einen (drohenden) Cyber-Vorfall nutze, der nicht versichert ist, muss ich die angefallenen Kosten für Crawford als Krisenmanager bezahlen?

W. R Berkley Europe AG übernimmt die Kosten für die Inanspruchnahme der Cyber-Krisenhotline und des Cyber-Krisenmanagers für Sie. Auch wenn sich später herausstellt, dass kein versichertes Schadenereignis vorliegt, kommen wir für die bis dahin entstandenen Kosten auf. Wichtig: Voraussetzung für die Kostenübernahme ist begründeter Cyber-Verdachtsfall.

Sind Crawford und die externen Netzwerkpartner unabhängig?

Ja. Sowohl Crawford als auch die Experten aus dem Cyber-Krisennetzwerk agieren unabhängig und neutral in der Cyber-Krisenbewältigung. Für die Durchführung und den Erfolg der Dienstleistungen ist W. R. Berkley Europe AG nicht verantwortlich. Eventuelle entstehenden Ansprüche sind direkt gegen den Dienstleister zu richten.

Kann ich einen Dienstleister verwenden, der nicht Netzwerkpartner von Crawford ist oder kein bevorzugter Krisenexperte ist?

W. R. Berkley Europe AG verfügt über ein weltweites Netzwerk aus erfahrenen und krisenerprobten Experten, u.a. aus den Bereichen IT-Forensik, PR-/Krisenkommunikation oder Datenschutz. Diese stehen für eine schnelle und zuverlässige Lösung eines Cyber-Krisenfalls. Als Versicherungsnehmerin profitieren Sie bei Beauftragung unserer Experten von attraktiven Sonderkonditionen. Die finale Auswahl des Expertennetzwerkes erfolgt durch Sie. Sofern Sie im Cyber-Krisenfall auf Ihre eigenen Dienstleister vertrauen möchten, ist dies jedoch unbedingt vorab mit uns zu vereinbaren – im Idealfall bei Vertragsabschluss. Auf diese Weise geht im Cyber-Krisenfall keine Zeit verloren und die Kostenübernahme kann durch uns verbindlich bestätigt und die abweichenden Dienstleister in der Police dokumentiert werden. Beziehen Sie unsere Experten aus dem Expertennetzwerk unverzüglich ein, da dies eine effektive und auch rechtssichere Bewältigung der Cyber-Krise für Sie erheblich vereinfacht und i.d.R. die Cyber-Krise besser koordiniert und beendet werden kann.

Wichtige zusätzliche Hinweise

1. Drucken Sie dieses Dokument aus und stellen Sie sicher, dass Sie jederzeit Zugriff hierauf haben.

2. Informieren und schulen Sie mehrere Personen in Ihrem Unternehmen, mindestens die IT-Abteilung, Rechtsabteilung und Datenschutzbeauftragte über den Prozess und die Cyber-Krisenhotline (u.a. wegen Abwesenheiten, Urlaub, Zuständigkeiten, etc.). Beziehen Sie die Geschäftsleitung mit ein.

3. Erstellen Sie einen internen Prozess und Berechtigungen zur Meldung des Cyber-Vorfalls bei Crawford, W. R. Berkley Europe und Ihrem Versicherungsmakler.

4. Spielen Sie das Szenario einer Schadenmeldung/Cyber-Vorfalls in Ihrem Unternehmen durch. Prüfen Sie diesen Prozess auch, wenn keine digitale Kommunikation möglich ist.

5. Beziehen Sie Crawford als Cyber-Krisenmanager unverzüglich in den Cyber-Vorfall ein.

6. Legen Sie eindeutig vorab fest, wer kommuniziert. Sprechen Sie mit „einer Stimme“.

7. Dokumentieren Sie den Cyber-Vorfall und sammeln Sie Fakten.

8. Klären Sie vorab die Thematik Datenschutz inkl. Zusammenarbeit mit Ihrem Datenschutzbeauftragen im Cyber-Krisenfall.

9. Verpflichten Sie alle Beteiligten zur Vertraulichkeit.

10. Bewahren Sie Ruhe und vertrauen Sie auf die Hilfe externer Cyber-Krisenexperten.

Kontaktdaten Ihres Versicherers

W. R. Berkley Europe AG	Tel.: +49 (0) 221 99386 0
Niederlassung für Deutschland	Fax: +49 (0) 221 37050048
Christophstraße 19	E-Mail: wrbvd_schaden_cyber@wrberkley.com
50670 Köln	Internet: www.berkleyversicherung.de

Hinweis
Die entsprechende 24/7/365 Telefon-Hotline sowie Hinweise zum Vorgehen im Cyber-Krisenfall werden in der Police dokumentiert.

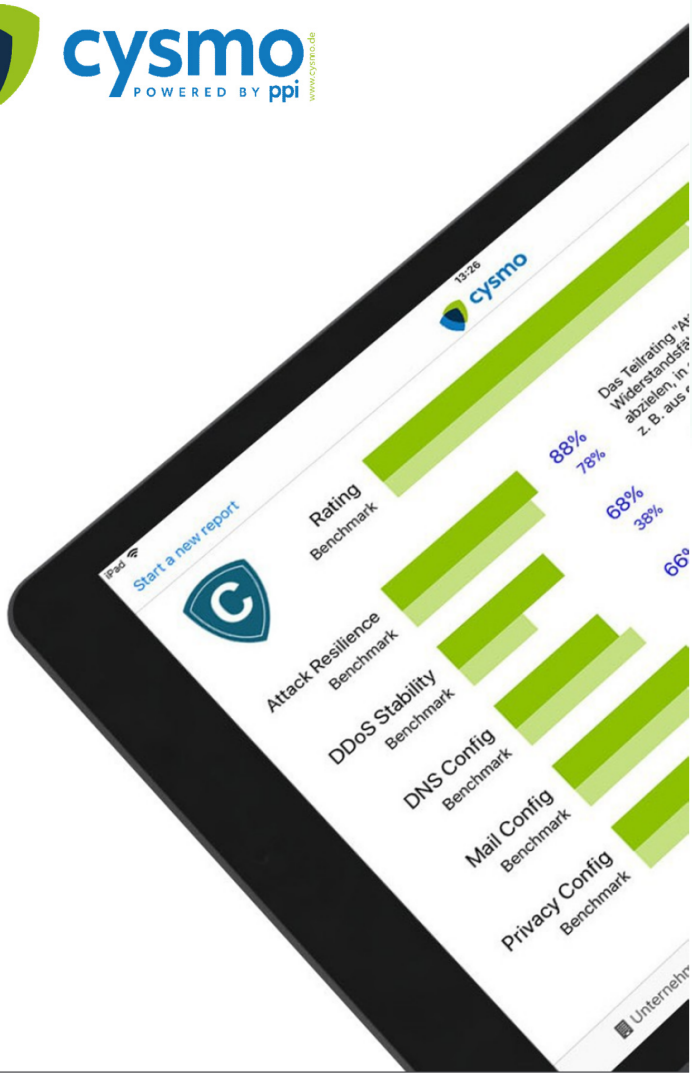
Realtime Cyber-Risikoanalyse mit cysmo®

Vollautomatisierte Cyber-Risikobewertung für die Kunden von Berkley Deutschland. Auf Knopfdruck. In Echtzeit.

Die neue Dimension in der Cyber-Risikobewertung.

cysmo® bewertet die Sicherheit der von außen sichtbaren IT-Infrastruktur eines Unternehmens. Die online öffentlich zugänglichen Systeme des Unternehmens werden geprüft und bewertet. Dabei orientieren sich die ausgefeilten cysmo®-Sicherheitskriterien an den Empfehlungen und Branchenstandards, etwa von BSI und VdS.

cysmo®-Bewertungen bilden die aktuelle Angreifbarkeit der IT-Infrastruktur eines Unternehmens als Momentaufnahme ab, das heißt, dass die Situation sich jederzeit ändern kann. cysmo® stellt keine umfängliche Risikobewertung für Cyberattacken dar, sondern zeigt vielmehr die IT-Angreifbarkeit aus Sicht eines Cyberkriminellen. Somit ist ein cysmo®-Rating als Bestandteil einer umfänglichen Risikoanalyse anzusehen, in der die Cyberrisiken Ihres Unternehmens ganzheitlich bewertet werden.



Realtime Cyber-Risikoanalyse mit cysmo®

Besonderheit für alle Cyber-Versicherungskunden von Berkley Deutschland:

Zum Vertragsabschluss und zur Vertragsverlängerung erhält jeder Cyber-Kunde den aussagekräftigen Risikoreport inkl. einer Management Summary mit Handlungsempfehlungen. Dies ist für Sie ein kostenloser Service.

Die von cysmo® erstellten Teilratings decken verschiedene potenzielle Schwachstellen einer Unternehmens-IT auf. Diese differenzierte Darstellung des Gesamtratings macht das Ergebnis für alle Beteiligten transparent und nachvollziehbar.

Attack Resilience

Ein Blick von außen auf das Unternehmen: Gibt es offene Zugänge oder sind interne Systeme sichtbar? Welche Angriffspunkte würde ein potentieller Angreifer sehen? Das Teilrating Attack Resilience stellt die nach außen sichtbare Angriffsoberfläche des bewerteten Unternehmens dar – ohne hierbei aktive Scans oder Penetrationen auf den Systemen oder Komponenten durchzuführen.

DDoS Stability

Jemand telefoniert zu viel auf einer Leitung? Gibt es Ersatzsysteme, die bei einem Teilausfall eingesetzt werden? Es ist empfehlenswert, eine Alternative zu haben. Das Teilrating DDos Stability verschafft einen Überblick über die Verteilung der IT-Infrastruktur nach außen. Es bewertet die Belastbarkeit der Infrastruktur hinsichtlich DDoS-Angriffen (Distributed Denial of Service).

DNS Config

Wurden alle erforderlichen Sicherheitsmaßnahmen getroffen, damit sich kein Angreifer unbefugten Zutritt zu den Systemen verschaffen kann? Oder sind vertrauliche Informationen vielleicht für jeden einsehbar ungeschützt und öffentlich zugänglich? Das Teilrating DNS Config bewertet die Konfiguration der genutzten DNS- Infrastruktur (Domain Name System), also derjenigen Server, die für die Namensauflösung der Systeme zuständig sind.

Mail Config

Sind versendete und empfangene Mails ausreichend vor dem Mitlesen durch Dritte geschützt? Werden Mails von Kunden vielleicht als Spam wahrgenommen? Das Teilrating *Mail Config* bewertet die Konfiguration der verwendeten Mailserver, etwa im Hinblick auf eine angemessene Verschlüsselung oder auf die Abwehr von Social-Engineering-Attacken.

Privacy and Reputation

Ist für eine ausreichende Sicherheit der Website-Besucher gesorgt? Sind ihre Daten und Privatsphäre umfänglich geschützt? Oder wird der Webauftritt des Unternehmens als Bedrohung wahrgenommen? Das Teilrating Privacy and Reputation bewertet das Benutzerverhalten (Tracking) von Website-Besuchern. Bewertet werden hierbei unter anderem Verschlüsselung, Vertraulichkeit und Weiterleitung von Benutzerdaten und Informationen an Dritte.

DarkNet

Sind E-Mail-Adressen der Mitarbeiter oder des Unternehmens in falsche Hände gelangt? Welche Gefahr verbirgt sich dahinter? Kann es zu einer Erpressung kommen? Sollten kurzfristig Schutzmaßnahmen ergriffen werden? Das Teilrating Darknet bewertet die Angriffsoberfläche bezüglich des Social Engineering auf Basis von Darknet-Informationen, die beispielsweise Unternehmensadressen aus öffentlichen Netzwerken berücksichtigen.

cysmo® unterstützt Berkley Deutschland und seine Versicherungskunden dabei, Cyberrisiken sichtbar zu machen und etwaige Sicherheitslücken schnell und effizient aufzuzeigen. Ein Mehrwert für alle Beteiligten – damit ein Cyberschaden gar nicht erst entsteht.

CrowdStrike Falcon: Endgerätetechnologie der nächsten Generation

Die Einführung einer wirksamen Lösung für den Endgeräteschutz ist eine wichtige Maßnahme zur Abwehr krimineller Akteure und ständig wechselnder komplexer Bedrohungen.

CrowdStrike Falcon ist eine Lösung für den Endgeräteschutz der nächsten Generation. Sie setzt auf eine ganze Reihe von ergänzenden Verfahren zur Peävention und Erkennung und hilft Ihnen, sich gegen ständig neue Ransomeware-Techniken zu schützen.

Die Falcon-Plattform umfasst Folgendes:

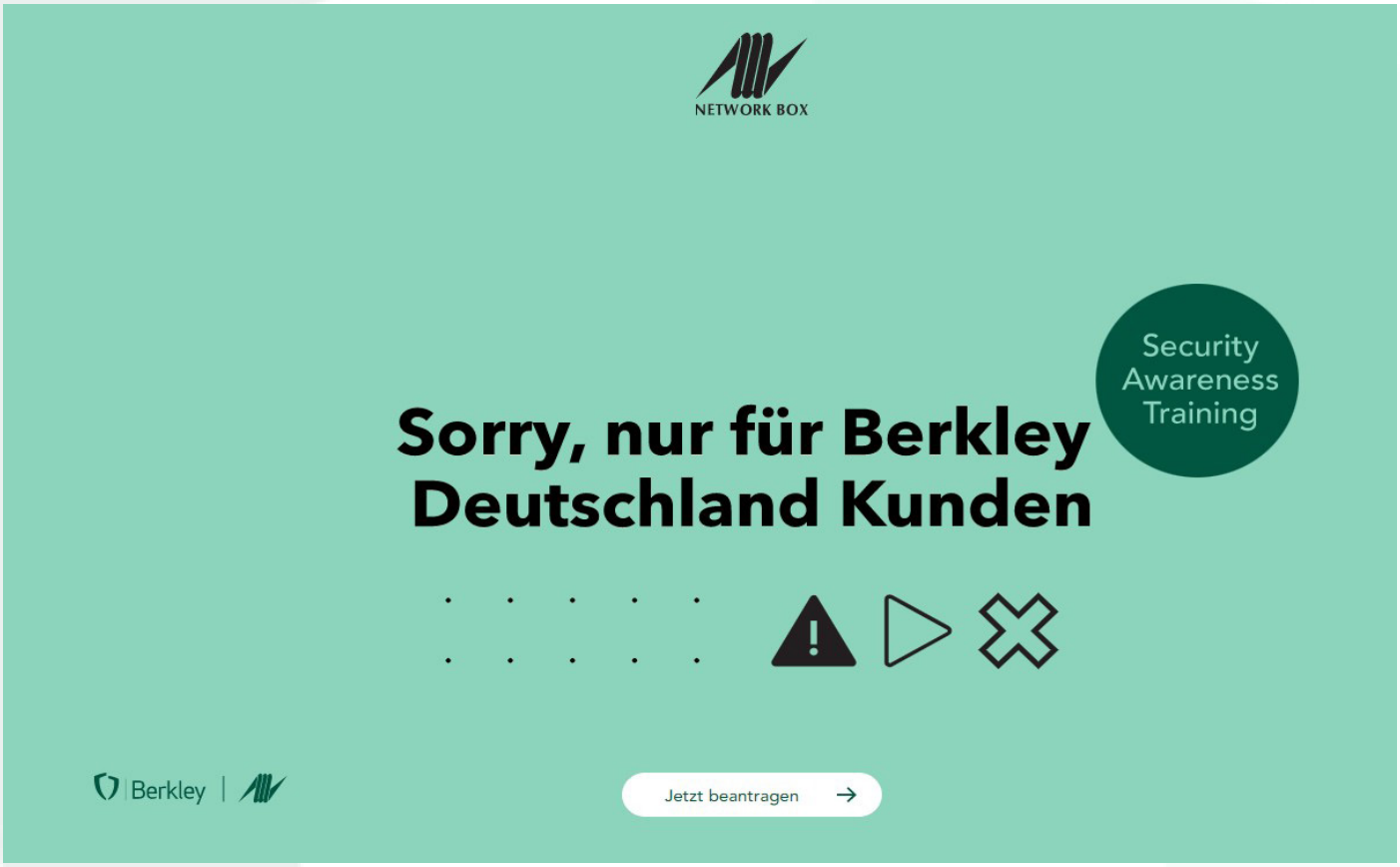
- ✓ Maschinelles Lernen zur Prävention bekannter und bisher unbekannter („Zero-Day“) Ransomware, ohne dass Updates erforderlich sind.
- ✓ Exploit Blocking als Schutz gegen die Ausführung und Verbreitung von Ransomware über nicht gepachtete Schwachstellen.
- ✓ Angriffsindikatoren (IOAs) zur Identifizierung und Blockierung krimineller Verhaltensweisen sowie zum Schutz gegen dateilose Angriffe und neue Ransomware-Kategorien.
- ✓ Automatisierte Bedrohungsanalyse zur sofortigen Ermittlung aller Details zur gefundenen Ransomware, wie beispielsweise Herkunft, Zuschreibung, Ähnlichkeiten und IOCs (Gefährdungsindikatoren).

DIE MODULE IM ÜBERBLICK	FALCON PRO	FALCON ENTERPRISE	FALCON PREMIUM	FALCON COMPLETE
FALCON PREVENT Antivirenlösung der nächsten Generation	✓	✓	✓	
FALCON X Bedrohungsaufklärung (Threat Intelligence)	+	+	+	
FALCON DEVICE CONTROL USB-Gerätesteuerung	+	+	+	
FALCON FIREWALL MANAGEMENT Firewall	+	+	+	
FALCON INSIGHT Endpunktbasierte Detektion und Reaktion (EDR)		✓	✓	
FALCON OVERWATCH Verwaltete Bedrohungssuche		+	+	
FALCON DISCOVER IT-Hygiene			✓	
CROWDSTRIKE SERVICES Incident Response und Proactive Services	OPTIONAL	OPTIONAL	OPTIONAL	

Vollständig verwalteter Endgeräteschutz – ein Service der Experten von CrowdStrike

Flexible Pakete: ✓ *im Lieferumfang* + *optionale Komponente*

Network Box



Die Hälfte aller **Cyberangriffe wird durch Mitarbeiter** versursacht. Mit einem Security Awareness Training schult IT-Sicherheitsspezialist Network Box aus Köln Ihre Mitarbeiter im richtigen Umgang mit E-Mails und Daten und sensibilisiert diese für Cyber-Risiken. Als Kunde der Berkley erhalten Sie das **Security Awareness Training** zu exklusiven Konditionen.

Network Box gehört zu den führenden IT-Sicherheitsspezialisten weltweit. Mit einem breiten Portfolio an monatlich kündbaren UTM-Lösungen über Security Awareness bis hin zu ganzheitlichen IT-Sicherheitskonzepten bietet der Hersteller und MSSP für jede Unternehmensgröße den passenden Schutz. Als Partner kooperieren wir mit Network Box im Bereich Prävention von Cyberangriffen.

Partnerschaften für unsere Cyber-Versicherungskunden

Berkley Deutschland bietet seinen Cyber-Versicherungskunden über **CrowdStrike** und **Network Box** die Möglichkeit, zusätzliche Cyber-Versicherungslösungen zu vergünstigten Konditionen einzukaufen.

Alle Links und Zugangsdaten zu den Plattformen unserer Partnerunternehmen erhalten Sie mit Abschluss Ihrer Berkley Cyber Risk Protect Versicherung. Bitte teilen Sie diese Informationen nicht, da dies ein spezielles Angebot für Cyber-Versicherungskunden von Berkley Deutschland ist.

Berkley Deutschland übernimmt keine Haftung aus den Dienstleistungen bzw. den bereitgestellten Services, die durch CrowdStrike und Network Box, der Versicherungsnehmerin angeboten werden.

Der Vertrag wird zwischen der Versicherungsnehmerin und CrowdStrike oder Network Box gschlossen. Berkley Deutschland hat keine Rechte und übernimmt daher keine Verpflichtungen aus dem Vertrag. Sämtliche Rechte und Pflichten aus solch einer Vereinbarung, insbesondere Rechnungen, Gebühren und Leistungen, gehen ausschließlich zu Nutzen und Lasten der Versicherungsnehmerin.

Versicherungskunden von Berkley Deutschland haben somit die Möglichkeit, Dienstleistungen bei CrowdStrike und Network Box über den entsprechenden Internetlink kostenpflichtig einzukaufen.

Bitte beachten Sie, dass dieser Service sich von Zeit zu Zeit ändern kann bzw. nicht mehr angeboten wird bzw. durch einen anderen ersetzt wird. Die Versicherungsnehmerin hat keinen Anspruch auf Bereitstellung eines derartigen Angebots durch den Versicherer.

Cyber-Versicherung

Informationsblatt zu Versicherungsprodukten

Unternehmen: W. R. Berkley Europe AG

Produkt:
Berkley Cyber Risk Protect

Dieses Blatt dient nur Ihrer Information und gibt Ihnen einen kurzen Überblick über die wesentlichen Inhalte Ihrer Versicherung.

Die vollständigen Informationen finden Sie in Ihren Vertragsunterlagen (Versicherungsantrag, Versicherungsschein und Versicherungsbedingungen). Damit Sie umfassend informiert sind, lesen Sie bitte alle Unterlagen durch.

Um welche Versicherung handelt es sich?

Es handelt sich um eine Vermögensschadenversicherung für Unternehmen zur Absicherung von Drittschäden, Eigenschäden, Datenschutzverfahren aufgrund eines Cyber-Vorfalls inklusive eines integrierten Cyber-Krisenmanagements.

Was ist versichert?

Unsere Versicherungslösung ist modular aufgebaut, so dass diese an Ihre individuellen Bedürfnisse angepasst werdenkann. Es wird u.a. Versicherungsschutz für folgende Cyber-Schäden gewährt:

- ✓ Cyber-Krisenmanagement
- ✓ Cyber-Eigenschäden
- ✓ Cyber-Drittschäden
- ✓ Cyber-Betriebsunterbrechung
- ✓ Datenschutzverfahren
- ✓ Entschädigungen mit Strafcharater, Bußgelder und Gebühren soweit rechtlich zulässig.

Wie hoch ist die Versicherungssumme?

- ✓ Die Höhe der vereinbarten Versicherungssummen können Sie Ihrem Antrag oder auch Ihrem Versicherungsschein entnehmen.

Was ist nicht versichert?

Wir können nicht alle denkbaren Fälle versichern, denn sonst müssten wir eine unangemessen hohe Prämie verlangen. Deshalb haben wir Fälle aus dem Versicherungsschutz herausgenommen.

Nicht versichert sind z.B.:

- X Vorsatz
- X Personen-/Sachschäden
- X Innenansprüche
- X Geistiges Eigentum
- X Bekannte Umstände und abhängige Verfahren
- X Ansprüche nach Ablauf der Nachmeldefrist

Gibt es Deckungsbeschränkungen?

In bestimmten Fällen ist der Versicherungschutz eingeschränkt, wie z.B.:

- ! Wir leisten für Cyber-Schäden nur bis zu der vereinbarten Versicherungssumme und Sublimiten. Wenn eine Selbstbeteiligung vereinbart ist, ist diese zu berücksichtigen.
- ! Folgende Versicherungsgegenstände sind standardmäßig mit einem Sublimit versehen:
  - ! Cyber-Erpressung
  - ! Cyber-Diebstahl
  - ! Datenschutzverfahren
  - ! Cyber-Betriebsunterbrechung bei Cloudausfall
  - ! Ansprüche in sog. Non-admitted Countries

Allgemeine Kundeninformationen

Informationen nach § 1 der Verordnung über Informationspflichten bei Versicherungsverträgen (VVG-InfoV)

1. Identität des Versicherers

W. R. Berkley Europe AG, Niederlassung für Deutschland
Hauptbevollmächtigter: José David Jiménez García

Wir sind eine Niederlassung der W. R. Berkley Europe AG,
Städtle 35a, 9490 Vaduz, Liechtenstein
Sitz der Niederlassung: Köln, Registergericht: Amtsgericht Köln HRB 85917

2. Vertreter in dem Mitgliedsstaat der EU

entfällt

3. Kontaktdaten und ladungsfähige Adresse der Niederlassung für Deutschland:

W. R. Berkley Europe AG:
Niederlassung für Deutschland:
Christophstraße 19:
50670 Köln:

Tel.: +49 (0) 221 99386 0
Fax: +49 (0) 221 37050048
E-Mail: wrbvd_info@wrberkley.com
Internet: www.wrberkley.de

Hauptbevollmächtigter für Deutschland: José David Jiménez García

4. Hauptgeschäftstätigkeit des Versicherers

Die W. R. Berkley Europe AG, Liechtenstein betreibt die Schaden-, Unfall- und Rückversicherung. Die deutsche Niederlassung betreibt aktuell die Bereiche Sach-, Haftpflicht-, D&O-, Unfall-, Cyber- und Sonderversicherungen.

5. Garantiefonds

entfällt

6. Wesentliche Merkmale der Versicherung

a) Dem Versicherungsverhältnis liegen die beigefügten Allgemeinen Vertragsbedingungen, etwaige weitere Besondere Bedingungen und Klauseln zugrunde.

b) Angaben über die Art, den Umfang, die Fälligkeit der Leistung des Versicherers entnehmen Sie bitte dem Antrag/der Deckungsaufgabe, dem Versicherungsschein, den detaillierten Versicherungsbedingungen sowie diesen Verbraucherinformationen.

7. Gesamtpreis der Versicherung

Die Versicherungsprämie wird auf der Grundlage der uns überlassenen Risikoinformationen, der vereinbarten Versicherungssumme sowie des vereinbarten Selbstbehaltes, berechnet. Die konkrete Höhe des Beitrags entnehmen Sie bitte dem Antrag/der Deckungsaufgabe und den Angaben im Versicherungsschein.

8. Zusätzlich anfallende Kosten

Im Falle einer Beitragsanmahnung berechnen wir für die Mahnung derzeit 5,00 EUR.
Kosten für Rücklastschriften, die vom Versicherungsnehmer oder dem Kontoinhaber verursacht wurden, fallen in Höhe der vom Bankinstitut im Einzelfall erhobenen Gebühren an.

9. Zahlung/Erfüllung/Zahlungsweise

Der Beitrag ist in der Regel an den in der Beitragsrechnung ausgewiesenen Empfänger zu zahlen. Weitere Einzelheiten zur Zahlungsweise des Beitrags entnehmen Sie bitte dem Versicherungsschein, den Allgemeinen Bedingungen, Besonderen Bedingungen/Vereinbarungen und Klauseln.

10. Befristung der Gültigkeitsdauer der Informationen

Angaben über die Gültigkeitsdauer entnehmen Sie bitte dem Antrag/der Deckungsaufgabe und dem beigefügten Versicherungsschein.

11. Spezifische Preismerkmale

entfällt

12. Zustandekommen des Vertrages

Der Versicherungsschutz beginnt, wenn der Vertrag abgeschlossen worden ist und der erste oder einmalige Beitrag rechtzeitig gezahlt wird; jedoch nicht vor dem mit Ihnen vereinbarten, in dem beigefügten Versicherungsschein angegebenen, Versicherungsbeginn.
Der Vertrag gilt als geschlossen, wenn wir Ihren Antrag auf Abschluss des Versicherungsvertrages angenommen haben bzw. wenn wir Ihre Annahmeerklärung zu unserem Antrag erhalten haben.

13. Widerrufsbelehrung/Widerrufsrecht

Widerrufsrecht

Sie können Ihre Vertragserklärung innerhalb von 14 Tagen ohne Angabe von Gründen in Textform (z. B. Brief, Fax, E-Mail) widerrufen. Die Frist beginnt, nachdem Sie den Versicherungsschein, die Vertragsbestimmungen einschließlich der Allgemeinen Versicherungsbedingungen, die weiteren Informationen nach § 7 Abs. 1 und 2 des Versicherungsvertragsgesetzes in Verbindung mit den §§ 1 bis 4 der VVG-InfoV und diese Belehrung jeweils in Textform erhalten haben. Zur Wahrung der Widerrufsfrist genügt die rechtzeitige Absendung des Widerrufs.

Der Widerruf ist zu richten an:

W. R. Berkley Europe AG,
Niederlassung für Deutschland,
Christophstraße 19 in 50760 Köln, oder
per Fax an +49 (0) 221 37050048, oder
per E-Mail an wrbvd_info@wrberkley.com

Widerrufsfolgen

Im Falle eines wirksamen Widerrufs endet Ihr Versicherungsschutz, und wir erstatten Ihnen den auf die Zeit nach Zugang des Widerrufs entfallenden Teil des Beitrages, wenn Sie zugestimmt haben, dass der Versicherungsschutz vor dem Ende der Widerrufsfrist beginnt. Den Teil des Beitrages, der auf die Zeit bis zum Zugang des Widerrufs entfällt, dürfen wir in diesem Fall einbehalten; dabei handelt es sich um einen Betrag in Höhe von 1/360 pro Tag des Jahresbeitrages, an dem Versicherungsschutz bestand. Die Höhe des Jahresbeitrages entnehmen Sie bitte dem Versicherungsschein. Die Erstattung zurückzuzahlender Beträge erfolgt unverzüglich, spätestens 30 Tage nach Zugang des Widerrufs. Beginnt der Versicherungsschutz nicht vor dem Ende der Widerrufsfrist, hat der wirksame Widerruf zur Folge, dass empfangene Leistungen zurückzugewähren und gezogene Nutzungen (z. B. Zinsen) herauszugeben sind.

Besondere Hinweise

Ihr Widerrufsrecht erlischt, wenn der Vertrag auf Ihren ausdrücklichen Wunsch sowohl von Ihnen als auch von uns vollständig erfüllt ist, bevor Sie Ihr Widerrufsrecht ausgeübt haben.
Das Widerrufsrecht besteht nicht bei Verträgen mit einer Laufzeit von weniger als einen Monat. Widerrufen Sie einen Ersatzvertrag, so läuft Ihr ursprünglicher Versicherungsvertrag weiter.

- Ende der Widerrufsbelehrung -

14. Laufzeit des Vertrages/Beendigung des Vertrages

Die Laufzeit des Vertrages beträgt in der Regel 12 Monate, es sei denn es wurde ausdrücklich etwas anderes vereinbart. In diesem Fall ist die Laufzeit dem Versicherungsschein zu entnehmen. Der Vertrag verlängert sich jeweils um ein weiteres Jahr, wenn er nicht von einer der Parteien unter Einhaltung der Kündigungsfrist von drei Monaten zum Ablauf der aktuellen Versicherungsperiode in Textform gekündigt wird. Daneben hat der Versicherungsnehmer die Möglichkeit, den Vertrag nach Eintritt eines Versicherungsfalls zu kündigen.

15. Abweichendes Recht der Vertragsanbahnung

entfällt

16. Anwendbares Recht / Vertragssprache /Gerichtsstand

Dem Vertrag – einschließlich der Verhandlungen vor Abschluss – liegt deutsches Recht zugrunde. Vertragssprache ist Deutsch. Ebenso erfolgt jede Kommunikation zwischen Ihnen und uns in Deutsch. Angaben zum zuständigen Gericht entnehmen Sie den beigefügten Versicherungsbedingungen.

17. Beschwerdemöglichkeit bei der Aufsichtsbehörde

Bei Fragen oder Beschwerden können Sie sich jederzeit direkt an unsere Kundenberatung wenden:

Kundenberatung
Tel: 0221 99386-0
Fax: 0221 37050048
E-Mail: **wrbvd_info@wrberkley.com**
Internet: **www.wrberkley.de**

Desweiteren können Sie Ihre Beschwerde auch an die zuständige Aufsichtsbehörde richten:
BaFin Bundesanstalt für Finanzdienstleistungsaufsicht,
Bereich Versicherungen,

Graurheindorfer Straße 108, 53117 Bonn.
Tel.: 0228 4108-0
Fax: 0228 4108-1550
E-Mail: **poststelle@bafin.de**

Weitere Einzelheiten finden Sie unter:
www.bafin.de

Versicherungsprodukte der Berkley Deutschland: Informationspflichten gemäß Art. 13 und Art. 14 der Datenschutzgrundverordnung (DSGVO) zum Datenschutz

Vorbemerkung:

Gerne möchten wir Sie gemäß der Datenschutzgrundverordnung (DSGVO) über die Verarbeitung Ihrer Daten durch W. R. Berkley Europe AG und die Ihnen nach dem Datenschutzrecht zustehenden Rechte im Rahmen der Inanspruchnahme unserer Versicherungsprodukte informieren.

Unsere jeweils aktuellste Datenschutzerklärung finden Sie hier: https://www.berkleyversicherung.de/datenschutz/.

1. Überblick

Zweck dieser Datenschutzerklärung ist es, Information darüber zur Verfügung zu stellen, wie die deutsche Niederlassung von W. R. Berkley Europe AG (im Folgenden: „Berkley Deutschland“) personenbezogene Daten erhebt, nutzt, verarbeitet, schützt und weitergibt, sowie welche Rechte insofern nach Maßgabe der Datenschutzgesetze bestehen.

Wenn in dieser Datenschutzerklärung von „wir“ oder „uns“ die Rede ist, sind damit Berkley Deutschland oder andere Unternehmen der W. R. Berkley Corporation gemeint. Weitere Informationen zu den Unternehmen der W. R. Berkley Corporation finden Sie hier: https://www.berkley.com/our-business/operating-units.

Wenn wir uns auf „Sie“ oder „Ihre“ beziehen, meinen wir Personen, deren Daten wir routinemäßig erfassen, z. B. Versicherte, Geschädigte oder andere an unseren Versicherungsprozessen Beteiligte.

2. Personenbezogene Daten, die wir verarbeiten

Um Ihnen eine Versicherung anbieten zu können oder Ihren Schadensfall zu bearbeiten, erheben wir gegebenenfalls die folgenden Kategorien personenbezogener Daten über Sie:

- Angaben zu Ihrer Person, wie Name, Adresse, Geburtsdatum, Kontaktdaten (einschließlich Ihrer Adresse, Telefonnummer und E-Mail-Adresse) und Geschlecht
- Informationen über Ihre Familie, Ihren Lebensstil und Ihre sozialen Verhältnisse, wie Familienstand, Angehörige und nächste Verwandte
- Informationen über Ihre finanziellen Verhältnisse und Ihre Bankverbindung (einschließlich des Namens Ihrer Bank und Ihrer Kontonummer)
- Informationen über Ihre Ausbildung und Beschäftigung/Arbeitsverhältnis, einschließlich Qualifikationen
- Informationen zur Identifizierung oder zu Background Checks (sofern gesetzlich zulässig), die für Ihre Police oder Ihren Schadensfall relevant sind

Für die Beurteilung Ihres Schadenfalls kann es auch erforderlich sein, dass wir sensible personenbezogene Daten erfassen und verarbeiten, z. B. medizinische Daten, die mit einem Unfall zusammenhängen. Die Rechtsgrundlage, auf die wir uns bei der Verarbeitung sensibler personenbezogener Daten stützen, finden Sie in Abschnitt 4 dieser Datenschutzerklärung.

3. Wie wir Ihre personenbezogenen Daten verwenden

Wir verwenden die über Sie gesammelten personenbezogenen Daten für die folgenden Zwecke:

Verwaltung unserer Policen und Verträge mit Ihnen

Wir müssen Ihre personenbezogenen Daten verarbeiten, damit wir unsere vertraglichen Verpflichtungen Ihnen gegenüber erfüllen können, einschließlich der Erstellung von Angeboten, der Zeichnung von Policen und der Bearbeitung von Schadensfällen. Dies kann die Weitergabe personenbezogener Daten an Dritte wie Schadensregulierer, Anwaltskanzleien, Wirtschaftsprüfer und Rückversicherer beinhalten.

Einhaltung aufsichtsrechtlicher oder anderer rechtlicher Anforderungen
Als Finanzdienstleistungsunternehmen sind wir von den Finanzaufsichtsbehörden autorisiert. In einigen Fällen werden wir personenbezogene Daten verarbeiten und an diese Aufsichtsbehörden weitergeben, um die an uns gestellten Anforderungen zu erfüllen.

Prävention und Aufdeckung von Betrug
Wir verarbeiten personenbezogene Daten, um Kontrollen zur Aufdeckung und Verhinderung von Betrug oder Finanzkriminalität durchzuführen, indem wir Informationen mit Kreditauskunfteien teilen oder öffentlich zugängliche Informationen nutzen.

Bereitstellung des Kundenservice
Wir verarbeiten personenbezogene Daten für unseren Kundenservice. Dies ermöglicht uns, Ihre Anfragen und Beschwerden zu bearbeiten. Diese Anfragen werden mitverfolgt und für spätere Zwecke gespeichert und können auch für interne Zwecke wie Qualitätssicherung und Schulungen verwendet werden.

Weitergabe personenbezogener Daten an andere Unternehmen der W. R. Berkley Corporation
Wir können Ihre personenbezogenen Daten an andere Unternehmen von W. R. Berkley Corporation weitergeben, um Ihre Police zu verwalten, Ihren Schadensfall zu bearbeiten oder für Zwecke der internen Unternehmensverwaltung und Berichtswesen.

Sie sind nicht verpflichtet, uns personenbezogene Daten zur Verfügung zu stellen. Sofern Sie dies aber nicht tun, kann das Auswirkung auf die Dienstleistungen haben, die wir Ihnen zur Verfügung stellen können. Weitere Informationen finden Sie im Abschnitt „Ihre Rechte“ weiter unten.

4. Rechtsgrundlage für die Verarbeitung personenbezogener Daten

Nach Datenschutzrecht dürfen wir Ihre personenbezogenen Daten nur dann verarbeiten, wenn wir eine entsprechende Rechtsgrundlage dafür haben. Für die Verarbeitung Ihrer personenbezogenen Daten stützen wir uns in der Regel auf die folgenden Rechtsgrundlagen:

Erfüllung unserer vertraglichen Verpflichtungen
Wir verarbeiten Ihre personenbezogenen Daten, um unsere vertraglichen Verpflichtungen zu erfüllen, die sich aus den mit Ihnen geschlossenen Verträgen ergeben.

Erfüllung gesetzlicher oder behördlicher Anforderungen
Wir können Ihre personenbezogenen Daten verarbeiten, wenn wir hierzu aufgrund geltender Gesetze und Vorschriften verpflichtet sind, wie z. B. solche, die sich auf die Verhinderung, Aufdeckung und Meldung von Betrug und anderen mit Finanzkriminalität verbundenen Angelegenheiten beziehen.

Legitimes Interesse
Wir können Ihre personenbezogenen Daten verarbeiten, wenn wir hieran ein berechtigtes Geschäftsinteresse haben, wobei wir sicherstellen, dass wir Ihre Interessen, Grundrechte und Grundfreiheiten schützen.

Einwilligung
Vor der Erhebung und/oder Verarbeitung sensibler personenbezogener Daten stellen wir sicher, dass wir Ihre ausdrückliche Einwilligung dazu haben oder uns auf eine Ausnahmeregelung berufen können, wie z.B. die Geltendmachung oder Verteidigung von Rechtsansprüchen durch uns oder Dritte.

5. Von wem werden personenbezogene Daten erhoben
Im Rahmen unserer Zeichnungs-, Policenverwaltungs- und Schadenbearbeitungsprozesse erheben wir personenbezogene Daten von Ihnen oder Ihrem Vertreter (z. B. Makler oder Vermittler). In der Regel werden diese Daten elektronisch, schriftlich oder mündlich erhoben. Wir können auch Informationen von folgenden Stellen einholen:

- in der Versicherungswirtschaft genutzte Register und Datenbanken
- beteiligten Parteien (z. B. Klägern, Geschädigte oder Zeugen)
- Kreditauskunfteien
- anderen öffentlich zugänglichen Quellen für Zwecke der Betrugsbekämpfung

6. Mit wem die Informationen geteilt werden
Für die in Abschnitt 3 dieser Datenschutzerklärung („Wie wir Ihre persönlichen Daten verwenden“) beschriebenen Zwecke können wir Ihre personenbezogenen Daten weitergeben an:

- andere Unternehmen der W. R. Berkley Corporation
- Bevollmächtigte Dritte oder Dienstleister, einschließlich Makler oder andere Versicherer für die Zwecke der Grund- oder Exzedentenversicherung und der Rückversicherung, sowie Drittanbieter und Anwälte für die Zwecke der Schadensregulierung.
- Regierungsstellen, Aufsichtsbehörden oder Behörden zur Verhinderung von Finanzkriminalität, um unseren gesetzlichen und aufsichtsrechtlichen Verpflichtungen nachzukommen.

Insofern, als wir Ihre personenbezogenen Daten an bevollmächtigte Dritte oder Dienstleister weitergegeben, stellen wir sicher, dass die notwendigen Sicherheitsvorkehrungen getroffen werden, um Ihre personenbezogenen Daten vor unbefugtem Zugriff, Offenlegung, Verlust oder Zerstörung zu schützen.

7. Datenübermittlung außerhalb des EWR
Wir sind auf globaler Ebene tätig. Daher kann es vorkommen, dass wir Ihre personenbezogenen Daten in Länder übermitteln, in denen andere Datenschutzgesetze gelten als im Europäischen Wirtschaftsraum („EWR“). Einige Länder außerhalb des EWR sind von der Europäischen Kommission als Länder anerkannt, die ein angemessenes Datenschutzniveau gemäß den EWR-Standards bieten (die vollständige Liste dieser Länder finden Sie hier: (Angemessenheitsbeschlüsse / Europäische Kommission (europa.eu)).

Für den Fall, dass personenbezogene Daten aus dem EWR in Länder übermittelt werden, für die kein Angemessenheitsbeschluss vorliegt, haben wir geeignete Maßnahmen ergriffen, wie z. B. die von der Europäischen Kommission erlassenen Standarddatenschutzklauseln, um Ihre personenbezogenen Daten zu schützen. Wenn Sie mehr über die Maßnahmen erfahren möchten, die wir zum Schutz Ihrer personenbezogenen Daten bei der Übermittlung ergriffen haben, können Sie sich mit uns wie in Abschnitt 12 beschrieben in Verbindung setzen.

8. Wie lange werden personenbezogene Daten aufbewahrt?
Wir bewahren Ihre personenbezogenen Daten nur so lange auf, wie sie gemäß unseren Aufbewahrungsrichtlinien für die in dieser Datenschutzerklärung genannten Zwecke benötigt werden, oder bis sie für gesetzliche, vertragliche, prozessuale oder behördliche Zwecke nicht mehr erforderlich sind. Danach werden Ihre personenbezogenen Daten vernichtet oder anonymisiert.

9. Marketing
Berkley Deutschland wird Ihre personenbezogenen Daten nicht für Marketingzwecke verwenden, es sei denn, wir haben Ihre Einwilligung hierzu erhalten.

10. Automatisierte Entscheidungsfindung
Wir können unter Verwendung Ihrer personenbezogenen Daten automatisierte Entscheidungen treffen. Prozesse, bei denen automatisierte Entscheidungen verwendet werden können, beziehen sich typischerweise auf:

- die Bestimmung von Preisen, Prämien und Zeichnungsentscheidungen, wenn Sie ein Angebot anfordern
- das Ausstellen einer Versicherungspolice
- die Prävention und Aufdeckung von Betrug
- die Ermöglichung der Prüfung von Sanktionen

11. Sicherheit
Wir sind bestrebt, angemessene organisatorische, technische und administrative Maßnahmen zu ergreifen, um personenbezogene Daten innerhalb unserer Organisation vor unbefugtem Zugriff, Missbrauch, Verlust oder Zerstörung zu schützen.

12. Ihre Rechte
Gemäß den geltenden Datenschutzgesetzen können Sie bestimmte Rechte in Bezug auf Ihre personenbezogenen Daten ausüben, einschließlich:

Auskunft	Sie können, vorbehaltlich bestimmter Ausnahmen, eine Kopie der personenbezogenen Daten, die wir über Sie gespeichert haben, anfordern. Wir dürfen hierfür Gebühren erheben, wenn die Anfrage als offenkundig unbegründet oder überzogen anzusehen ist.
Berechtigung	Sie können verlangen, dass wir Ihre personenbezogenen Daten aktualisieren oder berichtigen, um sicherzustellen, dass sie vollständig, richtig und aktuell sind.
Widerruf	Sie können uns auffordern, die Verarbeitung Ihrer personenbezogenen Daten einzustellen, wenn die Verarbeitung ausschließlich auf Ihrer Einwilligung beruht.
Widerspruch	Sie können der Verarbeitung Ihrer personenbezogenen Daten widersprechen. Wir werden entweder zustimmen oder erklären, warum wir der Bitte nicht nachkommen können. In diesem Fall sind wir möglicherweise nicht mehr in der Lage, weitere Dienstleistungen zu erbringen.
Löschung	Sie können uns auffordern, Ihre personenbezogenen Daten zu löschen, wenn diese nicht mehr benötigt werden oder es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt.
Einschränkung	Sie können uns unter bestimmten Umständen auffordern, die Verwendung Ihrer personenbezogenen Daten einzuschränken, z. B. wenn Sie der Meinung sind, dass die von uns gespeicherten personenbezogenen Daten unrichtig sind.
Datenübertragbarkeit	Sie können eine Kopie der personenbezogenen Daten, die Sie uns bereitgestellt haben, anfordern, damit Sie diese in einem übertragbaren Format für Ihre eigenen Zwecke verwenden können, z. B. um sie für ein anderes Unternehmen zu nutzen.

Wenn Sie von Ihren Rechten Gebrauch machten möchten, setzen Sie sich bitte mit uns wie in Abschnitt 13 beschrieben in Verbindung.

13. Weitere Fragen oder Beschwerden

Wenn Sie weitere Fragen zur Verarbeitung Ihrer personenbezogenen Daten haben oder eine Beschwerde im Zusammenhang mit der Verarbeitung Ihrer personenbezogenen Daten einreichen möchten, können Sie uns wie folgt kontaktieren:

W. R. Berkley Europe AG – Niederlassung für Deutschland
Christophstraße 19
50670 Köln
Telefon: +49 (0) 221 99386 0
E-Mail-Adresse: **DPO@wrberkley.com**

Sie haben zudem die Möglichkeit, sich mit Ihrer Beschwerde an die zuständige Datenschutzaufsichtsbehörde zu wenden:

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
Postfach 20 04 44
40102 Düsseldorf

Telefon: 0211/38424-0
Fax: 0211/38424-999
E-Mail: **poststelle@ldi.nrw.de**

www.ldi.nrw.de

Versicherungsbedingungen:
Berkley Cyber Risk Protect – Deutschland Stand 05.2022 Version Q Versicherungsmakler GmbH

Inhaltsverzeichnis

I. Versicherungsschutz für Schadenersatzansprüche Dritter 34
II. Versicherungsschutz bei Eigenschäden 35
III. Datenschutzverfahren 39
IV. Entschädigungen mit Strafcharakter, Bußgelder und PCI-Vertragsstrafen 39
V. Cyber-Krisenmanagement 40
VI. Erweitertes Cyber-Krisenmanagement 41
VII. Definitionen 42
VIII. Ausschlüsse 44
IX. Allgemeine Vertragsbedingungen 47

Hinweise

Die vorliegende Cyber-Versicherung der W. R. Berkley Europe AG bietet Versicherungsschutz für Drittschäden und Eigenschäden, die sich aus einem Cyber-Vorfall ergeben können, sowie Assistance-Leistungen im Bereich Cyber-Krisenmanagement.

Im Abschnitt I. „Versicherungsschutz für Schadenersatzansprüche Dritter“, Abschnitt III. „Datenschutzverfahren, Untersuchungen und Ermittlungen“ und Abschnitt IV. „Entschädigungen mit Strafcharakter, Bußgelder und PCI-Vertragsstrafen“ bietet dieser Cyber-Versicherungsvertrag Versicherungsschutz für Haftpflichtansprüche und Datenschutzverfahren, Untersuchungen und Ermittlungen auf Grundlage des Anspruchserhebungsprinzips („claims made“). Dies bedeutet, dass Versicherungsschutz dann bestehen kann, wenn ein Schadenersatzanspruch während der Laufzeit dieses Cyber-Versicherungsvertrags oder einer sich daran anschließenden Nachmeldefrist erstmalig geltend gemacht wird oder Datenschutzverfahren, Untersuchungen oder Ermittlungen in diesem Zeitraum eingeleitet werden.

Im Abschnitt II. „Versicherungsschutz bei Eigenschäden“ wird Versicherungsschutz auf Grundlage des Feststellungsprinzips gewährt. Eigenschäden sind danach versichert, sofern das versicherte Schadenereignis erstmalig innerhalb der Vertragslaufzeit festgestellt wird. Als Feststellung gilt die Kenntnis eines Repräsentanten der versicherten Unternehmen oder eines mitversicherten Unternehmens, welches keine Tochtergesellschaft ist.

Sämtliche Versicherungsleistungen, einschließlich Abwehr- und sonstige Kosten, werden auf die Versicherungssumme angerechnet. Sublimite sind in der Versicherungssumme enthalten.

Die Versicherungssumme wird im Versicherungsfall nicht durch den anzuwendenden Selbstbehalt verringert.

Für optionale Versicherungsgegenstände besteht nur Versicherungsschutz, wenn diese explizit im Versicherungsschein vereinbart sind und die Fragen im Antrag durch den Kunden mit „ja“ beantwortet wurden.

I. Versicherungsschutz für Schadenersatzansprüche Dritter

1. Gegenstand der Versicherung

Der Versicherer gewährt Versicherungsschutz für den Fall, dass Versicherte von Dritten aufgrund eines der nachfolgenden versicherten Schadenereignisse gemäß Ziffer I. 2. („Versicherte Schadenereignisse“) für einen Vermögensschaden basierend auf gesetzlichen Haftpflichtbestimmungen in Anspruch genommen werden. Dies gilt auch für verschuldensunabhängige Haftpflichtbestimmungen. Der Versicherungsschutz umfasst versicherte Schadenereignisse, die während der Vertragslaufzeit oder Rückwärtsversicherung eingetreten sind.

2. Versicherte Schadenereignisse

a) Informationssicherheitsverletzung

Eine Informationssicherheitsverletzung ist eine (i.) Datenschutzverletzung, (ii.) Netzwerksicherheitsverletzung, (iii.) Vertraulichkeitsverletzung.

i. Datenschutzverletzung

Eine Datenschutzverletzung ist jede Verletzung von geltenden Datenschutzbestimmungen. Eine Datenschutzverletzung kann aus einer gesetzlichen oder vertraglichen Verpflichtung hervorgehen. Zu den gesetzlichen Verpflichtungen zählen insbesondere das Bundesdatenschutzgesetz (BDSG), die Europäische Datenschutzgrundverordnung (EU-DSGVO) und vergleichbare inländische oder ausländische Rechtsnormen. Darüber hinaus ist ein Verstoß gegen eine selbst auferlegte unternehmensinterne Datenschutzrichtlinie eines Versicherten Unternehmens ebenfalls eine Datenschutzverletzung.

ii. Netzwerksicherheitsverletzung

Eine Netzwerksicherheitsverletzung ist jedes unbefugte Eindringen, jede unberechtigte Nutzung oder jeder unberechtigte Zugriff, jede unbefugte Verhinderung eines autorisierten Zugangs zum IT-System von Versicherten inklusive eines zielgerichteten oder nicht-zielgerichteten Hacker-Angriffs. Hierzu zählen insbesondere Phishing, die Veränderung, Zerstörung, Löschung, Veröffentlichung, Übertragung sowie das Kopieren und Ausspähen von (elektronischen) Daten bzw. Software, die sich auf dem IT-System von Versicherten befinden, sowie die Beanspruchung von dessen Systemressourcen (insbesondere Denial-of-Service-Attacken). Eine Netzwerksicherheitsverletzung umfasst auch die Übermittlung von Schadprogrammen (u.a. Viren und Trojaner) oder Denial-of-Service-Angriffe auf oder durch ein IT-System eines Versicherten auf Dritte.

iii. Vertraulichkeitsverletzung

Eine Vertraulichkeitsverletzung ist die unberechtigte Veröffentlichung, unberechtigte Nutzung oder der unberechtigte Zugriff auf vertrauliche Informationen, sofern sich die Daten im Verantwortungsbereich von Versicherten befinden.

b) Rechteverletzung durch digitale Medien

Der Versicherer gewährt vorbehaltlich Ziffer IX. 2. a) („Ergänzende Ausschlüsse“) im Falle einer Rechteverletzung durch digitale Medien Versicherungsschutz, sofern die Rechteverletzung durch eine Informationssicherheitsverletzung verursacht wurde. Eine Rechteverletzung durch digitale Medien ist die unbefugte Veröffentlichung, Weitergabe oder Verbreitung von digitalen Medieninhalten über das Internet inklusive der eigenen Internetpräsenz durch Versicherte oder durch Dritte im Auftrag eines Versicherten, die zu einer Rechteverletzung Dritter führt.

Eine Rechteverletzung liegt insbesondere in folgenden Fällen vor:

- Verletzung oder Beeinträchtigung von Persönlichkeitsrechten, Rufschädigung, Veröffentlichung von Informationen aus der Privatsphäre, kommerzielle Verwendung des Namens, Domainrechts oder Firmenrechts;
- Verletzung von geistigen Eigentumsrechten wie Urheberrechten, Geschmacksmusterrechten und Markenrechten (ohne Patente); Plagiate, widerrechtliche Verwendung oder Diebstahl von Ideen oder Informationen;
- Aus den beiden oben genannten Punkten resultierende Verstöße gegen das Wettbewerbsrecht.

c) Abhandenkommen, Beschädigung, Diebstahl oder Zerstörung des IT-Systems

Zusätzlich gilt die nachteilige Veränderung, der teilweise bzw. vollständige Verlust von Daten als unmittelbare Folge von Abhandenkommen, Beschädigung, Diebstahl, Unbrauchbarmachung, Veränderung oder Zerstörung des von Versicherten genutzten IT-Systems als Netzwerksicherheitsverletzung gemäß I. 2. a) ii.

d) Nicht angezeigte oder verspätete Benachrichtigung
Der Versicherer gewährt Versicherungsschutz für gesetzliche (insbesondere nach dem BDSG und der EU-DSGVO bzw. vergleichbaren ausländischen Rechtsnormen) und vertragliche Ansprüche von Dritten gegen Versicherte, sofern ein Vermögensschaden aufgrund einer verspäteten oder nicht erfolgten Anzeige einer Informationssicherheitsverletzung geltend gemacht wird.

e) Outsourcing-Dienstleister (Haftung)
Tritt eine Informationssicherheitsverletzung beim Outsourcing-Dienstleister (u.a. externe Datenverarbeitung für Versicherte) ein, der von Versicherten mit der Datenverarbeitung beauftragt wurde, gewährt der Versicherer für die ausgelagerte Datenverarbeitung Versicherungsschutz, sofern ein Versicherter hierfür gesetzlich einzustehen hat. Der Versicherungsschutz umfasst nicht die eigene gesetzliche Haftpflicht des Outsourcing-Dienstleisters sowie Regressansprüche des Outsourcing-Dienstleisters gegen Versicherte.

II. Versicherungsschutz bei Eigenschäden

1. Gegenstand der Versicherung

Der Versicherer gewährt Versicherungsschutz für Eigenschäden gemäß Ziffer II. 3. („Versicherte Eigenschäden“), die Versicherten aus oder in Zusammenhang mit einem versicherten Schadenereignis gemäß Ziffer II. 2. („Versicherte Schadenereignisse“) entstehen, die erstmalig während der Vertragslaufzeit festgestellt werden.

2. Versicherte Schadenereignisse

a) Informationssicherheitsverletzung gemäß Ziffer I. 2. a)

b) Bedienfehler
Bedienfehler ist der unsachgemäße oder die fehlerhafte Bedienung, Betrieb oder Einrichtung, Wartung und Aktualisierung des IT-Systems eines Versicherten oder die unbefugte Beschädigung, Zerstörung, Löschung, Verschlüsselung oder das Abhandenkommen von Daten durch fahrlässiges Handeln oder Unterlassen eines Versicherten, die/ der/ das eine Informationssicherheitsverletzung gemäß Ziffer I. 2. a) zur Folge hat.

c) Sachschaden an der Computer-Hardware von versicherten Unternehmen
Der Versicherer übernimmt die notwendigen und angemessenen Kosten für die Reparatur oder den Ersatz von Computer-Hardware versicherter Unternehmen, wenn diese unmittelbar und ausschließlich in Folge einer Netzwerksicherheitsverletzung beschädigt oder zerstört wird und somit nicht mehr für den ursprünglich beabsichtigten Zweck verwendet werden kann.

Dies beinhaltet auch die niedrigeren Kosten für die Reparatur, sofern wirtschaftlich sinnvoll und technisch möglich, oder alternativ den Ersatz bzw. Teil-Ersatz von physischen Komponenten der Computer-Hardware der versicherten Unternehmen. Der Ersatz erfolgt grundsätzlich durch Computer-Hardware gleicher Art und Qualität wie die beschädigte bzw. zerstörte Computer-Hardware abzüglich des Wertes des Altmaterials.

Es besteht kein Versicherungsschutz für Computer-Hardware von Dritten oder sogenannte „Bring your own device Geräte“ sowie in Folge von physischen Einwirkungen.

Der Ausschluss Personen-/ Sachschäden findet ausschließlich für den Versicherungsschutz unter dieser besonderen Bedingung keine Anwendung.

Es gilt ein Sublimit i.H.v. 50.000 EUR vereinbart.

3. Versicherte Eigenschäden

a) Wiederherstellungskosten

Wiederherstellungskosten sind die angemessenen und notwendigen Aufwendungen, die für die Reparatur, Wiederherstellung, Wiedergewinnung und Funktionsfähigkeit von Daten oder des IT-Systems von Versicherten anfallen. Hierzu zählt auch die Isolierung und Entfernung von Schadprogrammen. Voraussetzung ist, dass Versicherte die ausschließliche Kontrolle oder Zugriff auf das IT-System und die Daten haben. Hat der Versicherte nicht die ausschließliche Kontrolle oder Zugriff auf das IT-System und die Daten, besteht Versicherungsschutz für Wiederherstellungskosten, sofern das schadenauslösende versicherte Ereignis von dem Teilbereich des IT-Systems der Versicherten ausgeht, welches der vollständigen Kontrolle und alleinigen Herrschaftsgewalt der Versicherten unterliegt.

Soweit technisch möglich, wird der Datenbestand bzw. die Funktionsfähigkeit des IT-Systems der Versicherten wiederhergestellt, der vor dem versicherten Schadenereignis bestand. Es werden auch die angemessenen und notwendigen Kosten für die Nutzung von anzumietender IT, externer Dienstleister, Durchführung alternativer Arbeitsweisen gemäß einem Geschäftskontinuitätsplan sowie erhöhte Arbeitsaufwendungen übernommen. Dies umfasst auch die Neuinstallation von Software sowie die notwendigen Kosten für Softwarelizenzen, die zur Wiederherstellung der Daten bzw. Software erforderlich sind.

b) Cyber-Betriebsunterbrechung und Cyber-Ertragsausfallschaden

Der Versicherer gewährt Versicherungsschutz für Cyber-Ertragsausfallschäden und angemessene und notwendige Kosten, die sich aus einer Cyber-Betriebsunterbrechung für Versicherte ergeben.

i. Begriff der Cyber-Betriebsunterbrechung

Eine Cyber-Betriebsunterbrechung ist die vollständige oder teilweise Unterbrechung der Produktion oder die Reduzierung der Erbringung von Dienstleistungen von Versicherten, die unmittelbar aus einem versicherten Schadenereignis resultiert. Darüber hinaus besteht Versicherungsschutz für eine Cyber-Betriebsunterbrechung, welche unmittelbar durch eine Reparatur im Rahmen einer versicherten Wiederherstellung gemäß Ziffer II. 3. a) verursacht wird.

ii. Begriff des Cyber-Ertragsausfallschadens

Der Cyber-Ertragsausfallschaden berechnet sich aus dem Betriebsgewinn, den ein Versichertes Unternehmen während und infolge der Cyber-Betriebsunterbrechung nicht erwirtschaften kann und den fortlaufenden Kosten.

Im Rahmen der Cyber-Betriebsunterbrechung werden folgende Kosten nicht ersetzt:

- Aufwendungen für Roh-/ Hilfs- und Betriebsstoffe sowie bezogene Waren und Leistungen, soweit es sich nicht um Aufwendungen zur Betriebserhaltung oder um Mindest- und Vorhaltegebühren für Energiefremdbezug handelt;
- Umsatzsteuer, Verbrauchssteuern und Ausfuhrzölle;
- Umsatzabhängige Aufwendungen für Ausgangsfrachten;
- Umsatzabhängige Versicherungsprämien;
- Umsatzabhängige Lizenzgebühren und umsatzabhängige Erfindervergütungen;
- Gewinne und Kosten, die mit dem Fabrikations-, Handels-, Dienstleistungs- oder Gewerbebetrieb nicht zusammenhängen;
- Entschädigungen, soweit der Cyber-Ertragsausfallschaden durch außergewöhnliche und während der Cyber-Betriebsunterbrechung hinzukommende Ereignisse, erhöht wird. Es besteht weiterhin aber Versicherungsschutz, sofern diese Ereignisse nicht auf den ursprünglichen Versicherungsfall zurückzuführen sind;
- Verluste, die durch eine ungünstige Marktsituation verursacht werden.

iii. Beginn und Ende der Cyber-Betriebsunterbrechung

Beginn ist der Zeitpunkt, in welchem die Cyber-Betriebsunterbrechung eintritt. Ende ist der Zeitpunkt, ab welchem die Cyber-Betriebsunterbrechung nicht mehr besteht, das IT-System wiederhergestellt ist oder die im Versicherungsschein vereinbarte Haftzeit abläuft. Maßgeblich ist der Eintritt des frühesten Ereignisses.

iv. Haftzeit

Die Haftzeit ist der Zeitraum, für den der Versicherer für den Cyber-Ertragsausfallschaden aufgrund einer Cyber-Betriebsunterbrechung maximal leistet. Die Haftzeit beginnt mit Eintritt der Cyber-Betriebsunterbrechung und endet mit dem Ablauf der im Versicherungsschein vereinbarten Dauer.

v. Zeitlicher Selbstbehalt bei Cyber-Betriebsunterbrechung
Der zeitliche Selbstbehalt beginnt mit Eintritt der Cyber-Betriebsunterbrechung und endet nach Ablauf der im Versicherungsschein vereinbarten Dauer. Der Versicherer ersetzt den entstandenen Cyber-Ertragsausfallschaden nach Ablauf des vereinbarten zeitlichen Selbstbehaltes. Ein monetärer Selbstbehalt findet keine Anwendung.

vi. Berechnung des Cyber-Ertragsausfallschadens
Bei der Berechnung des Cyber-Ertragsausfallschadens werden alle Umstände (mit der Ausnahme ungünstiger Marktsituationen) berücksichtigt, die das Geschäftsergebnis positiv oder negativ beeinflusst hätten, wenn keine Cyber-Betriebsunterbrechung eingetreten wäre. Der Bewertungszeitraum sind die letzten 36 Monate vor Eintritt der Cyber-Betriebsunterbrechung. Der Bewertungszeitraum endet zum Zeitpunkt der Beendigung der Cyber-Betriebsunterbrechung gemäß Ziffer II. 3. b) iii).

Die Entschädigungsleistung durch den Versicherer darf zu keiner Bereicherung von Versicherten führen.

vii. Mehrkosten zur Wiederherstellung des Geschäftsbetriebes
Vorbehaltlich einer vorherigen Zustimmung durch den Versicherer in Schrift- oder Textform, die ausschließlich aus sachlichem Grund verweigert werden kann, besteht zusätzlich Versicherungsschutz für die angemessenen und notwendigen Mehrkosten, die für eine provisorische Aufrechterhaltung oder zur Beschleunigung der Wiederherstellung des Betriebes aufgewendet werden, um eine versicherte Cyber-Betriebsunterbrechung zu verkürzen oder zu verhindern. Mehrkosten sind Kosten, die zusätzlich zu den gewöhnlichen Kosten der Fortführung des Geschäftsbetriebs von Versicherten aufgewendet werden müssen. Angemessen sind Mehrkosten, wenn diese sich im Verhältnis zu den Kosten der Cyber-Betriebsunterbrechung als günstiger darstellen. Hierzu zählen Kosten für die Inanspruchnahme von Fremddienstleistungen, Kosten für die Nutzung fremder Anlagen oder eines IT-Systems Dritter, Kosten zur Information von Kunden oder Zulieferern, Kosten für Überstunden, Reisekosten, Zuschläge für Sonn-, Feiertags-, Nachtarbeit zur Nachholung für Produktion und Absatz, Wert von Vorräten, Ausgangsfracht, Stillstands-, Anlaufkosten sowie Kosten aufgrund von Abnahmeverpflichtungen wie Lagerungs- und Transportkosten.

viii. Forensische Buchhaltung
Zusätzlich gewährt der Versicherer Versicherungsschutz für die Unterstützung für forensischen Buchführungs- und Rechnungslegungskosten von Versicherten, um einen Cyber-Ertragsausfallschaden und die Schadenhöhe nachzuweisen.

Es gilt ein Sublimit i.H.v. 50.000 EUR vereinbart.

ix. Technische Probleme
Der Versicherer gewährt den Versicherten bei Cyber-Betriebsunterbrechungen zusätzlich Versicherungsschutz für entstandene Cyber-Ertragsausfallschäden infolge von technischen Problemen.

Technische Probleme sind Fehlfunktionen des IT-Systems von Versicherten, die weder durch das IT-System selbst, eine Fehlbedienung, Programmierfehler noch eine Informationssicherheitsverletzung entstehen.

Technische Probleme sind:
- Softwarefehler;
- Hardwarefehler;
- Interne Netzwerkfehler;
- Überhitzung;
- Elektrostatische Aufladung und statische Elektrizität;
- Fehlfunktion infolge eines Ausfalls der Stromversorgung, sofern diese unter der unmittelbaren Kontrolle von Versicherten ist.

Technische Probleme infolge des Ausfalls oder Beeinträchtigung von externen Infrastrukturen, die nicht der Kontrolle von Versicherten unterliegen, sind ausgeschlossen.

Es gilt ein Sublimit i.H.v. 250.000 EUR vereinbart.

x. Ausfall externer IT-Dienstleistungen

Der Versicherer gewährt den Versicherten bei Cyber-Betriebsunterbrechungen zusätzlich Versicherungsschutz für entstandene Cyber-Ertragsausfallschäden infolge des unvorhergesehenen Ausfalls bzw. der Nichtverfügbarkeit von externen IT-Dienstleistungen (u.a. Cloud-Dienste, ausgelagertes IT-System) durch eine Informationssicherheitsverletzung gemäß Ziffer I. 2. a). Voraussetzung ist, dass die Versicherten die Leistung der externen IT-Dienstleister für die Bearbeitung, Speicherung, Wartung oder Hosting entgeltlich und auf Basis einer schriftlichen Vereinbarung in Anspruch nehmen und der externe IT-Dienstleister kein Versichertes Unternehmen gemäß diesen Versicherungsbedingungen ist.

Die Nutzung von „Software as a Service" (SaaS), „Platform as a Service" (PaaS) und „Infrastructure as a Service" (IaaS) gilt als externe IT-Dienstleistung. Zudem besteht Versicherungsschutz für ein IT-System, welches von einem Dritten für Versicherte auf Basis eines schriftlichen Nutzungsvertrages zur Nutzung bereitgestellt wird.

Es gilt ein Sublimit i.H.v. 250.000 EUR vereinbart.

c) Cyber-Erpressung

Der Versicherer gewährt den Versicherten im Falle einer tatsächlichen oder angedrohten Cyber-Erpressung Versicherungsschutz für das Cyber-Krisenmanagement (gemäß Ziffer V.) und die Zahlung von Cyber-Erpressungsgeld.

Eine Cyber-Erpressung ist eine rechtswidrige Drohung gegen Versicherte mit einer Informationssicherheitsverletzung und der zeitgleichen Forderung von Cyber-Erpressungsgeld für die Nicht-Umsetzung der Drohung. Der Versicherungsschutz umfasst auch die Zahlung von Cyber-Erpressungsgeld, um die Veröffentlichung von vertraulichen Informationen zu verhindern bzw. die Freigabe von verschlüsselten IT-Systemen bzw. Daten, die sich im Verantwortungsbereich von Versicherten befinden, zu erwirken.

Cyber-Erpressungsgeld ist jede Form von Geld inklusive Kryptowährungen, Waren und Dienstleistungen. Sofern das Cyber-Erpressungsgeld in Form einer Kryptowährung, von Waren oder Dienstleistungen geleistet wird, erstattet der Versicherer den jeweiligen Gegenwert in EURO zum Übergabezeitpunkt (es gilt Ziffer X. 13. „Fremdwährung" entsprechend). Die Wiedererlangung von Cyber-Erpressungsgeld durch die Versicherten ist unverzüglich dem Versicherer anzuzeigen und das Cyber-Erpressungsgeld ist, soweit es durch den Versicherer getragen wurde, zurückzuerstatten.

Es gilt ein Sublimit i.H.v. 50% der Versicherungssumme bzw. maximal 1 MEUR vereinbart.

d) Cyber-Kriminalität

Der Versicherer gewährt den Versicherten Versicherungsschutz für unmittelbare Vermögensschäden durch die unberechtigte Nutzung oder den unberechtigten Zugang Dritter zum IT-System von Versicherten. Der Versicherer ersetzt hierbei die folgenden entstandenen Vermögensschäden:

- Erhöhte Kosten und Nutzungsentgelte durch die widerrechtliche Nutzung von Anwendungen wie Telekommunikationsanlagen oder Voice-Over-IP;
- Verlust von Geld, Buchgeld/ Giralgeld, Kryptowährung, Wertpapieren sowie unautorisierte Zahlungen und Überweisungen, die beispielweise durch die Manipulation von Online-Zahlungssystemen, Online-Banking oder Anwendungsprogrammen erfolgen; Dies gilt für Geld, Buchgeld/ Giralgeld, Kryptowährungen und Wertpapiere nur, sofern ein Versicherter für den Verlust gesetzlich haftet.
- Den Warenwert von verloren gegangenen (Handels-) Waren produziert von Versicherten durch unautorisierte (Aus-) Lieferung durch Versicherte.

Darüber hinaus besteht Versicherungsschutz für angemessene und notwendige externe Kosten für die Durchsetzung von Schadenersatzansprüchen gegen den Schadenverursacher (hierzu zählen u.a. Rechtsanwaltskosten sowie Gerichts-/ Verfahrenskosten).

Es besteht kein Versicherungsschutz, sofern die unberechtigte Nutzung oder der unberechtigte Zugang zum IT-System von Versicherten Dritten mit Unterstützung oder Duldung durch Versicherte ermöglicht wurde oder Versicherten die unberechtigte Nutzung oder der unberechtigte Zugang bekannt war. Mittelbar entstandene Schäden wie CEO-Fraud/ Fake-President-Schäden sind ausdrücklich nicht vom Versicherungsschutz umfasst.

Es gilt ein Sublimit i.H.v. 250.000 EUR vereinbart.

III. Datenschutzverfahren

1. Gegenstand der Versicherung

Der Versicherer gewährt Versicherungsschutz für den Fall, dass gegen Versicherte aufgrund eines versicherten Schadenereignisses (gemäß Ziffer III. 2.) ein versichertes Datenschutzverfahren, Untersuchungen oder Ermittlungen gemäß Ziffer III. 3. eingeleitet wird. Der Versicherungsschutz umfasst versicherte Schadenereignisse, die während der Vertragslaufzeit oder Rückwärtsversicherung eingetreten sind.

2. Versichertes Schadenereignis

a) Informationssicherheitsverletzung gemäß Ziffer I. 2. a)

3. Versicherte Eigenschäden

b) Behördliche Ermittlungen und Verfahren

Der Versicherer gewährt Versicherungsschutz für die externen angemessenen und notwendigen Verteidigungskosten im Falle der Einleitung eines Straf- oder Ordnungswidrigkeitsverfahrens gegen Versicherte aufgrund einer Informationssicherheitsverletzung.

c) Interne Untersuchungen und Ermittlungen

Der Versicherer gewährt Versicherungsschutz für die intern anfallenden notwendigen und angemessenen Kosten, wenn von einer Behörde, dem Datenschutzbeauftragten oder einer anderen internen Abteilung eines Versicherten Unternehmens eine interne Ermittlung hinsichtlich einer Informationssicherheitsverletzung mit dem Zweck zur Prüfung der Notwendigkeit einer Selbstanzeige, zur Vorbereitung der Selbstanzeige oder zur Durchführung einer Selbstanzeige angeordnet oder gefordert wird. Die internen Kosten werden übernommen, sofern diese Kosten in vergleichbarer Höhe auch bei Beauftragung eines externen Unternehmens entstanden wären.

Es gilt ein Sublimit i.H.v. 50.000 EUR vereinbart.

d) Consumer Redress Fund

Sofern im Zusammenhang mit behördlichen Verfahren oder internen Untersuchungen wegen einer Informationssicherheitsverletzung eine Geld-Einzahlung in sogenannte Consumer Redress Funds rechtlich verpflichtend erforderlich wird, wird diese Einzahlung vom Versicherer übernommen. Voraussetzung ist, dass durch diese Einzahlung Ansprüche von Verbrauchern gegen Versicherte befriedigt werden, die aufgrund einer bei Versicherten eingetretenen Informationssicherheitsverletzung bestehen.

Es gilt ein Sublimit i.H.v. 100.000 EUR vereinbart.

IV. Entschädigungen mit Strafcharakter, Bußgelder und PCI-Vertragsstrafen

In Ergänzung zum Versicherungsschutz nach Ziffer I. und III. gewährt der Versicherer Versicherungsschutz unter den nachfolgenden Voraussetzungen auch für Entschädigungen mit Strafcharakter, Bußgelder und Vertragsstrafen.

Es gilt ein Sublimit i.H.v. 50% der Versicherungssumme bzw. maximal 1 MEUR vereinbart.

1. Entschädigung mit Strafcharakter

Sofern rechtlich zulässig, gewährt der Versicherer den Versicherten gemäß Ziffer I. 1. auch Versicherungsschutz für Entschädigungen mit Strafcharakter (punitive damages, exemplary damages und vergleichbare Entschädigung), wenn diese einem Versicherten aufgrund einer Informationssicherheitsverletzung gemäß Ziffer I. 2. a) durch eine Behörde oder Gericht bestands- oder rechtskräftig auferlegt werden.

2. Bußgelder

Sofern rechtlich zulässig, gewährt der Versicherer den Versicherten gemäß Ziffer III. 1. auch Versicherungsschutz für Bußgelder, wenn diese einem Versicherten von einer staatlichen Datenschutzbehörde oder einem Gericht aufgrund einer Datenschutzverletzung gemäß Ziffer I. 2. a) bestands- oder rechtskräftig auferlegt werden.

3. Payment Card Industry (PCI)-Vertragsstrafen

Der Versicherer gewährt Versicherten gemäß Ziffer I. 1. auch Versicherungsschutz für Vertragsstrafen infolge einer eingetretenen Informationssicherheitsverletzung gemäß Ziffer I. 2. a), die sich aus der Verletzung des Payment Card Industry Data Security Standards (PCI DSS) ergeben. Der Versicherungsschutz beinhaltet darüber hinaus die notwendigen und angemessenen Kosten für den Nachweis der PCI-Compliance und die weiteren an den Vertragspartner zu zahlenden Gebühren (z.B.: Kartenneuausstellung und Übernahme der Kosten des Betruges).

Zusätzlich ist die fortgesetzte Nichteinhaltung des Payment Card Industry Data Security Standard für einen Zeitraum von bis zu drei (3) Monaten ab dem Tag der ersten Feststellung (im Sinne von Ziffer X. 4 b)) der Nichteinhaltung versichert, solange die Versicherten nachweisen, an der Wiederherstellung der Einhaltung zu arbeiten.

V. Cyber-Krisenmanagement

Sofern Versicherungsschutz nach Ziffer I. 1., II. 1. oder III. 1. besteht, gewährt der Versicherer den jeweiligen Versicherten weiter Unterstützung beim Cyber-Krisenmanagement nach dieser Ziffer V. für die nachfolgend genannten angemessenen und notwendigen Kosten. Sofern Cyber-Krisen-Dienstleister aus dem Berkley Deutschland-Netzwerk oder andere mit dem Versicherer vorab individuell und in Schrift- oder Textform vereinbarte Dienstleister beauftragt werden, ist keine Abstimmung hinsichtlich der Auswahl der Dienstleister mit dem Versicherer notwendig.

1. Cyber-Krisenberater

Der Versicherer übernimmt die Kosten der Beauftragung des Cyber-Krisenberaters für die Koordinierung des versicherten Schadenereignisses mit den Cyber-Krisen-Dienstleistern und den Versicherten. Zusätzlich steht der Cyber-Krisenberater den Versicherten als direkter Ansprechpartner zur Verfügung. Die entsprechenden Kontaktdaten des Cyber-Krisenberaters sind im Versicherungsschein und auf der Homepage der W. R. Berkley Europe AG hinterlegt.

2. IT-Forensik/ IT-Spezialisten

Der Versicherer übernimmt die Kosten für die Beauftragung von externen IT-Spezialisten und IT-Beratern zur Ursachenerforschung, Schadenfeststellung und -ausmaß, Identifizierung von Betroffenen, Ermittlung von negativen Folgen, gerichtsverwertbaren Beweissicherung und für geeignete Maßnahmen zur Schadenminderung im Zusammenhang mit einem versicherten Schadenereignis. Darüber hinaus werden die angemessenen und notwendigen Kosten für eine Sicherheitsanalyse und Empfehlungen für Sicherheitsverbesserungen in Bezug auf die für das versicherte Schadenereignis ursächliche Sicherheitslücke übernommen.

3. Reputationskosten

Der Versicherer übernimmt die Kosten für die Beauftragung eines externen PR-Beraters oder Kommunikationsberaters für die interne und externe Krisenkommunikation, Erstellung und Durchführung einer PR-Strategie und gegebenenfalls eines Mediencoachings sowie die Platzierung von Medienveröffentlichungen zur Wahrung oder Wiederherstellung der Reputation von Versicherten in Bezug auf Glaubwürdigkeit, Vertrauenswürdigkeit, Verantwortung und Zuverlässigkeit. Dies beinhaltet auch Medienveröffentlichungen im Falle eines nicht erfolgten oder falsch dargestellten versicherten Schadenereignisses bei Versicherten sowie, falls erforderlich, dessen mediale Nachbereitung.

4. Rechtsberatung

Der Versicherer übernimmt die Kosten für die Beauftragung einer externen Rechtsberatung zur rechtlichen Prüfung des zugrundeliegenden versicherten Schadenereignisses inklusive der Prüfung der geltenden Anzeige- und Meldepflichten sowie Handlungsempfehlungen zur weiteren rechtlichen Vorgehensweise sowie um negative Folgen des versicherten Schadenereignisses zu mindern oder zu vermeiden. Hiervon umfasst sind auch die Kosten für gerichtliche Maßnahmen für eine Unterlassungsklage oder zwecks Widerruf einer falschen öffentlichen Berichterstattung über ein versichertes Schadenereignis bei Versicherten.

VI. Erweitertes Cyber-Krisenmanagement

Ergänzend zu Ziffer V. gewährt der Versicherer den jeweiligen Versicherten Unterstützung beim Erweiterten Cyber-Krisenmanagement nach dieser Ziffer VI. für die nachfolgend genannten angemessenen und notwendigen Kosten.

1. Benachrichtigungskosten

Der Versicherer übernimmt die Kosten für die gesetzlich oder vertraglich notwendigen Benachrichtigungskosten von Betroffenen, Kunden und Behörden infolge einer erfolgten Informationssicherheitsverletzung gemäß Ziffer I. 2. a) bei Versicherten. Hierzu zählen unter anderem die Informationsaufbereitung, Erstellung und Versand von Informationsschreiben, Anzeigenschaltung, Ermittlung und Einrichtung eines Call-Centers zur Beantwortung von Rückfragen von Betroffenen und Kunden. Auf Wunsch von Versicherten, umfasst dies auch die freiwillige Benachrichtigung von Betroffenen, Kunden und Behörden, sofern dies für die Cyber-Krisenbewältigung sinnvoll ist.

2. Schadenminderung

Der Versicherer übernimmt die Kosten für die aufgewendeten notwendigen und angemessenen Schadenminderungskosten zur Minderung oder Vermeidung eines versicherten Schadenereignisses, sofern Versicherte diese nach Abwägung der Umstände als erfolgversprechend und angemessen halten durften. Der Versicherungsschutz beinhaltet in diesem Fall auch die erfolglos aufgewendeten Schadenminderungskosten.

Es gilt ein Sublimit i.H.v. 10% der Versicherungssumme bzw. maximal 1 MEUR vereinbart.

3. E-Discovery

Der Versicherer übernimmt die Kosten für die Beauftragung von IT-Dienstleistungen, um einer Aufforderung einer Behörde oder eines Gerichts zur Herausgabe von elektronisch gespeicherten Informationen in Folge einer Informationssicherheitsverletzung (u.a. UK Civil Procedure Rules 31 und US Regel 26 (b) (1) Federal Rules of Civil Procedure) oder Verletzung des Payment Industry Data Security-Standards (PCI DSS) zu entsprechen.

Es gilt ein Sublimit i.H.v. 100.000 EUR vereinbart.

4. Datenrettung/ -sicherung

Der Versicherer übernimmt die externen Kosten zur Feststellung der zu rettenden/ sichernden Daten sowie der Schadenhöhe in Folge einer Informationssicherheitsverletzung, die nicht im Zusammenhang mit einer Cyber-Betriebsunterbrechung stehen.

5. Freiwillige Selbstanzeige

Der Versicherer übernimmt die Kosten, die einem Versicherten aufgrund einer freiwilligen Selbstanzeige bei einer inländischen oder ausländischen Datenschutzbehörde wegen eines tatsächlichen oder vermuteten versicherten Schadenereignisses entstehen. Voraussetzung für eine Kostenübernahme ist eine vorherige Abstimmung mit dem Versicherer sowie eine Abstimmung mit dem Cyber-Krisenberater in Schrift- oder Textform.

Es gilt ein Sublimit i.H.v. 50.000 EUR vereinbart.

6. Monitoring

Der Versicherer übernimmt die externen Kosten von Versicherten für Monitoring-Dienstleistungen hinsichtlich Dritter, die unmittelbar von einer bei Versicherten eingetretenen Informationssicherheitsverletzung betroffenen sind. Zu den Monitoring-Dienstleistungen zählen u.a. Kreditüberwachungsdienst-/ Kreditschutzleistungen, rechtlich oder gesetzlich verpflichtende Datenüberwachungsdienstleistungen sowie die laufende Beobachtung, Beurteilung und Auswertung von Konten von Betroffenen. Dies umfasst auch die Überwachung von sozialen Medien, Überwachung von Identitätsdiebstahl, Aufwendungen für Betrugspräventionssoftware für Privatpersonen sowie Kosten für die Eröffnung neuer Bankkonten von Betroffenen. Der Versicherungsschutz wird bereits bei Anhaltspunkten für einen Missbrauch der personenbezogenen Daten infolge der Informationssicherheitsverletzung bei Versicherten gewährt, sofern die Daten dazu verwendet werden können, im Namen der Betroffenen Verträge abzuschließen, Bankkonten zu eröffnen oder neue Kreditkarten zu beantragen. Die Monitoring-Dienstleistungen werden für die Betroffenen für einen Zeitraum von bis zu zwölf (12) Monaten ab Feststellung (im Sinne von Ziffer X. 4b)) der Informationssicherheitsverletzung gewährt.

Goodwill-Aktionen

a) Kostenerstattung für Vorbereitung
Der Versicherer übernimmt die Kosten der Erstellung, Verteilung, Frankierung und des Versandes von Goodwill-Aktionen (Preisnachlässe, Gutscheine und Rabatte, etc.) für die von einer bei Versicherten eingetretenen Informationssicherheitsverletzung betroffenen Dritten.

VII. Definitionen

1. Vermögensschäden
Vermögensschäden sind solche Schäden, die weder Personenschäden (Tötung, Körperverletzung oder Schädigung der Gesundheit von Personen) noch Sachschäden (Beschädigung, Verderben oder Vernichtung oder Abhandenkommen von Sachen) sind noch sich unmittelbar aus solchen Schäden herleiten. Als Sachen gelten insbesondere auch Geld, geldwerte Zeichen oder sonstige in Wertpapiere verbriefte Vermögenswerte.

Im Sinne dieser Versicherungsbedingungen gelten der Verlust, die Veränderung, Blockade oder Nichtverfügbarkeit von elektronischen als auch physischen Daten als Vermögensschaden. Dies schließt auch immaterielle Schäden (insbesondere Persönlichkeitsrechtsverletzungen Dritter) ein.

2. Versicherte
Versicherte sind die Versicherten Unternehmen gemäß Ziffer VIII. 3 und deren Mitversicherte Personen gemäß Ziffer VIII. 4. Darüber hinaus besteht auch Versicherungsschutz für explizit im Versicherungsschein genannte mitversicherte Unternehmen, die keine Tochtergesellschaften der Versicherungsnehmerin sind. Sofern für einzelne Vertragsbestandteile explizit vereinbart, zählen hierzu auch Outsourcing-Dienstleister.

3. Versicherte Unternehmen
Versicherte Unternehmen sind die Versicherungsnehmerin gemäß Versicherungsschein und deren direkte oder indirekte Tochtergesellschaften.

a) Begriff der Tochtergesellschaft
Tochtergesellschaften sind juristische Personen sowie vergleichbare Gesellschaftsformen nach ausländischem Recht, bei denen die Versicherungsnehmerin:

- Mehr als 50% der Stimmrechte der Gesellschafter hält;
- Das Recht hat, die Mehrheit der Mitglieder des Verwaltungs-, Aufsichtsrats oder sonstigen Leitungsorganen zu bestellen oder abzurufen und gleichzeitig mit mindestens 25% der Stimmrechte Gesellschafter ist;
- Aufgrund eines geschlossenen Beherrschungsvertrages oder aufgrund Satzungsbestimmung beherrschenden Einfluss auf dieses Unternehmen hat;
- Bei wirtschaftlicher Betrachtung die Mehrheit der Risiken und Chancen eines Unternehmens trägt, das zur Erreichung eines eng begrenzten und genau definierten Ziels der Versicherungsnehmerin dient (Zweckgesellschaft). Dies schließt auch sonstige juristische Personen des Privatrechts oder unselbständige Sondervermögen des Privatrechts ein. Ausgenommen sind aber Spezial AIF im Sinne des § 1 Abs. 6 Kapitalanlagegesetzbuch (KAGB) oder;
- Direkt oder indirekt die Mehrheit der Kapitalanteile hält.

b) Neu hinzukommende Tochtergesellschaften

i. Automatischer Einschluss

Wird während der Vertragslaufzeit eine neue Gesellschaft durch Erwerb oder Gründung zu einer Tochtergesellschaft der Versicherungsnehmerin, so ist diese automatisch ab dem Erwerb bzw. der Gründung vom Versicherungsschutz umfasst. Abweichend von Satz 1 erfolgt kein automatischer Einschluss für:

- Gesellschaften mit Sitz in den USA/ Kanada;
- Finanzdienstleistungsunternehmen (gemäß §§ 1 Abs. 1 und 4; 1a, 1b Versicherungsaufsichtsgesetz (VAG), § 1 Absatz (1b) Kreditwesengesetz (KWG) sowie vergleichbare Unternehmen nach deutschem bzw. ausländischem Recht);
- Telekommunikationsunternehmen, IT-Service-Provider, Cloud-Service-Provider
- Gesellschaften mit einem konsolidierten Umsatz von mehr als 30% des zuletzt geprüften konsolidierten Umsatzes der Versicherungsnehmerin.

ii. Vorsorgedeckung

Für neu hinzukommende Tochtergesellschaften, die nicht automatisch vom Versicherungsschutz gemäß Ziffer VIII. 3. b) i. umfasst sind, besteht vorsorglicher Versicherungsschutz für einen Zeitraum von sechzig (60) Tagen ab Erwerb bzw. Gründung. Die Versicherungsnehmerin ist verpflichtet, den Versicherer über die neue Tochtergesellschaft innerhalb von dreißig (30) Tagen nach Erwerb bzw. Gründung in Schrift- oder Textform zu informieren. Der Versicherer wird den Einschluss der Gesellschaft anhand von angeforderten Risikoinformationen innerhalb von maximal dreißig (30) Tagen nach Erhalt dieser Unterlagen prüfen. Der Versicherer ist berechtigt, den endgültigen Einschluss von einer Bedingungs- und Prämienanpassung abhängig zu machen.

Sofern die Gesellschaft dauerhaft in den Vertrag eingeschlossen wird, besteht ab dem Zeitpunkt der Gründung bzw. des Erwerbes rückwirkend Versicherungsschutz. Ist der Einschluss nicht möglich bzw. wird keine Einigung über den Einschluss erzielt, endet der vorsorgliche Versicherungsschutz automatisch rückwirkend und etwaige erbrachte Versicherungsleistungen sind zu erstatten.

c) Ausscheidende Tochtergesellschaften

Verliert eine Gesellschaft die Voraussetzungen einer Tochtergesellschaft gemäß Ziffer VIII. 3. a), endet der Versicherungsschutz für diese Gesellschaft ab diesem Zeitpunkt automatisch.

4. Mitversicherte Personen

Mitversicherte Personen sind:

- Die gesetzlichen Vertreter eines Versicherten Unternehmens;
- Die Personen in Leitungsfunktionen eines Versicherten Unternehmens;
- Die übrigen angestellten Mitarbeiter eines Versicherten Unternehmens;
- Die in den Betrieb eingegliederten Mitarbeiter von Zeitarbeitsunternehmen eines Versicherten Unternehmens;
- Die in den Betrieb eingegliederten freien Mitarbeiter aus ihrer Tätigkeit für ein versichertes Unternehmen;
- Die o.g Personen von Tochtergesellschaften und explizit im Versicherungsschein genannten mitversicherten Unternehmen.

5. Repräsentanten

Als Repräsentanten der Versicherten Unternehmen gelten:

- Die Inhaber (Einzelfirmen);
- Die Geschäftsführer (bei Gesellschaften mit beschränkter Haftung);
- Die Mitglieder des Vorstandes (bei Vereinen, Aktiengesellschaften, Versicherungsvereinen auf Gegenseitigkeit);
- Die Komplementäre (bei offenen Handelsgesellschaften sowie bei Gesellschaften bürgerlichen Rechts);
- Bei anderen Unternehmensformen (wie z.B. Kommunen, Körperschaften des öffentlichen Rechts, Verbänden, Körperschaften) die nach den gesetzlichen Vorschriften berufenen obersten Vertretungsorgane;
- Bei Gesellschaften nach ausländischem Recht die den vorgenannten Personen entsprechenden Personen;
- Die Leiter der IT-Abteilung, der Leiter Rechtsabteilung und der Leiter des Risikomanagements sowie der Chief Information Security Officer (CISO) sowie die vorgenannten Personen mit gleicher Verantwortung.

Den Versicherten wird ausschließlich das Wissen, der Vorsatz sowie Handlungen und Unterlassungen der Repräsentanten der Versicherungsnehmerin und mitversicherten Gesellschaften, die keine Tochtergesellschaften sind, zugerechnet.

6. Dritte

Dritte sind sämtliche natürliche und juristische Personen, die nicht Versicherte gemäß Ziffer VIII. 2. sind und die nicht ein Recht eines Versicherten im eigenen Namen oder einen Anspruch aus abgetretenem Recht eines Versicherten geltend machen. Mitversicherte Personen, die durch eine Informationssicherheitsverletzung gemäß Ziffer I. 2. a) selbst betroffen sind, gelten in diesem Fall ebenfalls als Dritte.

7. IT-System von Versicherten Unternehmen

Unter IT-System sind Computer-Hardware und -Software sowie alle Systeme, auf welche über das Internet, Intranet, Extranet, Virtual Private Networks (VPN) zugegriffen werden kann, zu verstehen. Hierzu zählen insbesondere darauf gespeicherte Daten, angeschlossene Ein- und Ausgabegeräte, angeschlossene Speichermedien, mobile Geräte (insbesondere Laptop, Tablet, Handy, Smartphone), Netzwerkequipment, Firmware und Geräte, die der Datensicherung dienen. Sogenannte „Bring your own device“ Geräte von Mitversicherten Personen sind ebenfalls vom Versicherungsschutz umfasst. Zusätzlich gelten auch Embedded Systems, ICS-Systeme (Industry Control Systems), SCADA-Systeme (Supervisory Control And Data Acquisition Systems) und andere industrielle Automationssysteme als IT-System. Im Sinne dieser Bedingungen ist jedes IT-System, das von Versicherten betrieben, gemietet oder sich in deren Eigentum befindet, umfasst.

VIII. Ausschlüsse

1. Allgemeine Ausschlüsse

a) Vorsatz und wissentliche Pflichtverletzung

Es besteht kein Versicherungsschutz aufgrund von oder im Zusammenhang mit einer vorsätzlichen Schadenverursachung, wissentlichen Informationssicherheitsverletzung oder durch wissentliches Abweichen von Gesetzen, Vorschriften, Bedingung oder Anweisung des Auftraggebers oder einer Pflichtverletzung durch Repräsentanten von versicherten Unternehmen oder Outsourcing-Dienstleistern selbst oder mit deren Kenntnis.

Ist der Vorsatz oder die Wissentlichkeit streitig, wird Versicherungsschutz für Abwehrkosten bei Schadenersatzansprüchen Dritter (gemäß Ziffer I.) gewährt, bis eine rechtskräftige Feststellung von Vorsatz oder Wissentlichkeit in einem Haftpflicht- oder Deckungsprozess, einem Strafverfahren oder einem sonstigen behördlichen Verfahren oder ein Eingeständnis erfolgt. Sofern eine rechtskräftige Feststellung oder ein Eingeständnis vorliegt, entfällt der Versicherungsschutz rückwirkend und die bis dahin vom Versicherer geleisteten Kosten sind vollständig zurückzuerstatten.

b) Strafbare Handlungen

Es besteht kein Versicherungsschutz infolge strafbarer Handlungen Repräsentanten. Es besteht jedoch Versicherungsschutz, solange die strafbare Handlung nicht rechtskräftig festgestellt ist. Erfolgt eine solche Feststellung, entfällt der Versicherungsschutz rückwirkend und dem Versicherer sind die bis dahin von ihm aufgewandten Kosten zurückzuerstatten.

c) Vertragliche Haftung

Es besteht kein Versicherungsschutz für Haftpflichtansprüche, soweit diese aufgrund vertraglicher Vereinbarung oder besonderer Zusage über den Umfang der gesetzlichen Haftpflicht hinausgehen, sofern explizit nichts Anderes vereinbart ist. Dieser Ausschluss gilt jedoch nicht für die Haftung aus einer Vertraulichkeitsverletzung und für Payment Card Industry (PCI)-Vertragsstrafen.

d) Personen- und Sachschäden

Es besteht kein Versicherungsschutz aufgrund von oder im Zusammenhang mit Personen-/ Sachschäden.

e) Kartell- und Wettbewerbsrecht

Es besteht kein Versicherungsschutz für Verletzungen aufgrund von oder im Zusammenhang mit der Verletzung von Kartell- oder Wettbewerbsrechts. Dieser Ausschluss findet keine Anwendung auf den Versicherungsschutz bei einer Rechteverletzung durch digitale Medien gemäß Ziffer I. 2 b).

f) Geistiges Eigentum
Es besteht kein Versicherungsschutz für Verletzungen aufgrund von oder im Zusammenhang mit Patentrechtsverletzungen, Plagiaten, Markenrechten, Urheberrechten sowie anderem geistigen Eigentums.

Dieser Ausschluss findet keine Anwendung auf den Versicherungsschutz bei einer Rechteverletzung durch digitale Medien gemäß Ziffer I. 2 b).

g) Betriebs-/ Geschäftsgeheimnisse
Es besteht kein Versicherungsschutz für Verletzungen aufgrund von oder im Zusammenhang mit Betriebs-/ Geschäftsgeheimnissen. Dieser Ausschluss findet keine Anwendung bei einer Vertraulichkeitsverletzung gemäß Ziffer I. 2. a) iii.

h) Innenansprüche
Es besteht kein Versicherungsschutz für Ansprüche von Versicherten selbst oder zwischen Versicherten.

i) Bekannte Umstände und anhängige Verfahren
Es besteht kein Versicherungsschutz für oder im Zusammenhang mit Umständen, Schadenersatzansprüchen Dritter, Eigenschäden, Entschädigungen mit Strafcharakter, Bußgeldern und PCI-Vertragsstrafen sowie eingeleiteten bzw. anhängigen behördlichen oder gerichtlichen Verfahren oder (internen) Untersuchungen, die zu einem Versicherungsfall führen könnten, sofern diese den Versicherten bei Beginn des Versicherungsschutzes bekannt waren oder hätten bekannt sein müssen.

j) Krieg, feindliche Handlungen oder staatliche Maßnahmen; Cyber-Terrorismus
Es besteht kein Versicherungsschutz aufgrund von oder in Zusammenhang mit Krieg, feindlichen Handlungen oder staatlichen Maßnahmen.

Krieg, feindliche Handlungen oder staatliche Maßnahmen sind:

- Streiks, Unruhen oder ähnliche Arbeitskampfhandlungen;
- Krieg oder kriegsähnliche Handlungen (unabhängig davon, ob der Krieg erklärt wurde oder nicht); Terrorismus;
- Handlungen durch, im Namen oder zur Unterstützung eines souveränen Staates;
- Bürgerkrieg, Invasion oder Feindseligkeiten, Aufruhr, Volksaufstand oder Militärputsch, Revolte, Rebellion, Revolution, militärische oder widerrechtliche Machtergreifung;
- die Beschlagnahme, Verstaatlichung oder Zerstörung oder Beschädigung von Eigentum, einschließlich Daten, personenbezogene Daten, Dokumenten, IT-Equipment, IT-Systeme, Computer-Systeme, Software, Applikationen, Programme, Lizenzen, und ausgelagerter Datenverarbeitung-/ Speicherung auf Anordnung einer Regierung oder einer anderen Behörde;

oder alle Maßnahmen, die zur Verhinderung oder Abwehr der oben genannten Punkte A. bis E. ergriffen werden, ob physisch oder unter Verwendung eines IT-/ Computer Systems.

Dieser Ausschluss gilt nicht für Cyber-Terrorismus.

Cyber-Terrorismus ist jede gegen ein IT-System gerichtete Handlung einer Einzelperson oder einer Gruppe von Personen, die

(i) durch soziale, ideologische, religiöse, wirtschaftliche oder politische Ziele motiviert ist; oder
(ii) mit dem Ziel begangen wird, eine Regierung oder die Zivilbevölkerung bzw. Teile hiervon einzuschüchtern oder zu nötigen oder Bereiche der Wirtschaft bzw. die Volkswirtschaft zu beinträchtigen; vorausgesetzt, dass der Begriff Cyber-Terrorismus keine derartigen Aktivitäten umfasst, die auf Krieg, feindlichen Handlungen oder staatlichen Maßnahmen beruhen, daraus resultieren, darauf zurückzuführen sind oder in irgendeiner Weise damit verbunden sind.

k) Finanzmarkttransaktion
Es besteht kein Versicherungsschutz für Schäden aufgrund von oder im Zusammenhang mit einer unberechtigten Ausführung von Handelsgeschäften durch Versicherte aufgrund der Überschreitung von Vollmachten (unauthorized Trading) und jede Form des Kaufs oder Verkaufs von Anleihen, Derivaten, Devisen, Rohstoffen, Wertpapieren oder vergleichbaren Wertanlagen.

l) Widerrechtlich erhobene Daten und Daten ohne Nutzungsberechtigung
Es besteht kein Versicherungsschutz aufgrund von oder im Zusammenhang mit wissentlich unrechtmäßig erhobenen Daten durch Repräsentanten oder mit Wissen von Repräsentanten. Dies schließt Daten und Programme ein, zu deren Nutzung der Versicherte nicht berechtigt ist.

m) Infrastruktur/ Internet
Es besteht kein Versicherungsschutz wegen Schäden aufgrund von oder in Zusammenhang mit jeder Art von Störung oder Unterbrechung von:

- Gas- und Ölleitungen;
- Stromleitungen;
- Internetverbindungen/ -leitungen;
- Kabelleitungen;
- Satellitenverbindungen;
- Telekommunikationsleitungen bzw.-verbindungen;

sofern die Störung oder Unterbrechung nicht im unmittelbaren Kontrollbereich der Versicherten liegt.

2. Ergänzende Ausschlüsse
Die ergänzenden Ausschlüsse gelten ausschließlich für den jeweils aufgeführten Versicherungsgegenstand.

a) Rechteverletzung durch digitale Medien
Im Rahmen von Ziffer I. 2. b) besteht kein Versicherungsschutz für Haftpflichtansprüche wegen:

- Fehlerhafter Produktbeschreibungen: Fehlerhafte Produktbeschreibung ist eine unrichtige oder unvollständige Beschreibung von Dienstleistungen oder Produkten (insbesondere Preisangaben, Beschaffenheitsangaben, Inhaltsstoffe, etc.).
- Fehlerhafte Finanzdaten: Fehlerhafte Finanzdaten sind fehlerhafte, unrichtige oder unvollständige Veröffentlichungen von Finanzdaten (insbesondere Geschäftsberichte, Bilanzen, Kapitalmarktinformationen etc.).
- Verbreitung unerwünschter Korrespondenz bzw. Werbung: Verbreitung unerwünschter Korrespondenz bzw. Werbung ist die unaufgeforderte oder ungebetene Korrespondenz bzw. Kommunikation in physischer oder digitaler Form. Hierzu zählen insbesondere E-Mails zu Werbezwecken, Telefaxe, Telemarketing und Direktwerbung.

b) Cyber-Betriebsunterbrechung
Im Rahmen von Ziffer II. 3. b) besteht kein Versicherungsschutz:

i. Staatliche Maßnahmen
Es besteht kein Versicherungsschutz aufgrund eines Ausfalls des IT-Systems eines Versicherten aufgrund von oder in Zusammenhang mit einer Beschlagnahme, Verstaatlichung, Zerstörung oder sonstigen Maßnahme einer Behörde oder einer anderen staatlichen Institution, soweit die staatliche Maßnahme nach dem Recht des jeweiligen Landes rechtmäßig ist.

ii. Ungünstige Marktsituation
Es besteht kein Versicherungsschutz für Verluste, die infolge einer ungünstigen Marktsituation entstehen.

iii. Optimierungs-/ und Wartungsarbeiten
Es besteht kein Versicherungsschutz aufgrund von oder in Zusammenhang mit geplanten Wartungsarbeiten des IT-Systems oder geplanten Abschaltungen sowie einer geplanten Erneuerung oder einem geplanten Austausch des IT-Systems. Hierzu zählt auch die Behebung von Softwarefehlern und Sicherheitslücken.

c) Cyber-Erpressung
Im Rahmen von Ziffer II. 3. c) besteht kein Versicherungsschutz aufgrund von oder in Zusammenhang mit:

- Produkterpressung: Eine Drohung/ Erpressung, hergestellte, verarbeitete oder vertriebene Erzeugnisse eines versicherten Unternehmens zu (ver-)ändern oder zu kontaminieren.
- Repräsentanten: Eine Cyber-Erpressung oder sonstige betrügerische oder kriminelle Handlungen durch Repräsentanten.

IX. Allgemeine Vertragsbedingungen

1. Räumlicher Geltungsbereich und non-admitted-Countries
Es besteht weltweiter Versicherungsschutz, soweit dies rechtlich zulässig ist. Sofern dies aufgrund von lokalen gesetzlichen Regelungen nicht zulässig ist (z.B. „non-admitted“ Verbote), werden Versicherungsleistungen aus diesem Versicherungsvertrag ausschließlich gegenüber der Versicherungsnehmerin an deren Sitz erbracht.

2. Zeitliche Bestimmungen

a) Beginn und Ende der Versicherung/ Kündigungsfrist
Es besteht Versicherungsschutz ab dem im Versicherungsschein festgelegten Zeitpunkt. Der Versicherungsvertrag ist für die im Versicherungsschein festgelegte Dauer abgeschlossen (Versicherungsperiode).

Der Versicherungsvertrag verlängert sich stillschweigend um zwölf (12) Monate, wenn er nicht spätestens drei (3) Monate vor Ablauf der Versicherungsperiode durch eine Vertragspartei in Schrift- oder Textform gekündigt wird.

Infolge des Eintritts nachfolgender Ereignisse endet der Versicherungsschutz automatisch zum Ablauf der jeweiligen Versicherungsperiode, ohne dass es einer Kündigung bedarf:

- Neubeherrschung der Versicherungsnehmerin;
- Eröffnung des Insolvenzverfahrens über die Versicherungsnehmerin;
- Liquidation der Versicherungsnehmerin;
- Verschmelzung der Versicherungsnehmerin auf ein anderes Unternehmen;

b) Rückwärtsversicherung
Bei den Versicherungsgegenständen gemäß Ziffer I. („Versicherungsschutz für Schadenersatzansprüche Dritter“), Ziffer III. („Datenschutzverfahren, Untersuchungen und Ermittlungen“) und Ziffer IV. („Entschädigungen mit Strafcharakter, Bußgelder und PCI-Vertragsstrafen“) besteht Versicherungsschutz auch für vor Beginn der Vertragslaufzeit eingetretene Versicherte Schadenereignisse, die den Versicherten bis zum Versicherungsbeginn nicht bekannt waren oder hätte bekannt sein müssen.

c) Nachmeldefrist

i. Automatische Nachmeldefrist
Für drei (3) Jahre nach Beendigung des Versicherungsvertrages besteht eine prämienneutrale Nachmeldefrist für Versicherte Schadenereignisse, die während der Dauer des Versicherungsvertrages oder der Rückwärtsversicherung eintreten. Während der Nachmeldefrist besteht Versicherungsschutz im Rahmen und Umfang der Versicherungsbedingungen und in der Höhe des nicht verbrauchten Teils der Versicherungssumme der letzten Versicherungsperiode. Für die Versicherungsnehmerin besteht darüber hinaus die Möglichkeit, eine prämienpflichtige Nachmeldefrist von bis zu insgesamt fünf (5) Jahren einzukaufen.

ii. Keine automatische Nachmeldefrist:
In den folgenden Fällen besteht keine automatische Nachmeldefrist:

- Nichtzahlung der Versicherungsprämie ganz oder anteilig zum Zeitpunkt des Ablaufs der letzten Versicherungsperiode;
- Neubeherrschung der Versicherungsnehmerin;
- Eröffnung des Insolvenzverfahrens über die Versicherungsnehmerin;
- Liquidation der Versicherungsnehmerin;
- Verschmelzung der Versicherungsnehmerin.

3. Versicherungsfall

a) Versicherungsfall bei Drittschäden
Bei Drittschäden gemäß Ziffer I. (Versicherungsschutz für Schadenersatzansprüche Dritter"), Ziffer III. („Datenschutzverfahren, Untersuchungen und Ermittlungen") und Ziffer. IV. („Entschädigungen mit Strafcharakter, Bußgelder und PCI-Vertragsstrafen"), ist der Versicherungsfall die erstmalige Geltendmachung eines Haftpflichtanspruchs oder erstmalige Einleitung von versicherten Datenschutzverfahren, Untersuchungen oder Ermittlungen gegen einen Versicherten während der Dauer des Versicherungsvertrages oder einer anschließenden Nachmeldefrist nach Maßgabe von Ziffer X. 2. c). Im Sinne dieses Cyber-Versicherungsvertrages ist ein Haftpflichtanspruch geltend gemacht, wenn von einem Dritten gegen Versicherte ein Anspruch in Textform erhoben oder diesem gegenüber schriftlich mitgeteilt wird, einen Anspruch gegen einen Versicherten zu haben.

b) Versicherungsfall bei Eigenschäden
Im Rahmen der Eigenschäden gemäß Ziffer II. Versicherungsschutz bei Eigenschäden besteht Versicherungsschutz für Versicherte Schadenereignisse, die erstmalig während der Vertragslaufzeit festgestellt werden. Als Feststellung gilt die Kenntnis eines Repräsentanten der Versicherungsnehmerin oder eines mitversicherten Unternehmens, welches keine Tochtergesellschaft ist.

c) Cyber-Verdachtsfall und Rückforderungsverzicht beim Cyber-Krisenmanagement
Im Rahmen des Cyber-Krisenmanagements gemäß Ziffer V. besteht bereits im Falle eines begründeten Verdachts für ein versichertes Schadenereignis Versicherungsschutz. Dies schließt die Prüfung zur Feststellung eines versicherten Schadenereignisses ein. Die genannten Assistance-Leistungen des Cyber-Krisenmanagements werden ab der ersten Kontaktaufnahme mit dem im Versicherungsschein angegebenen oder individuell im Versicherungsschein vereinbarten Cyber-Krisenberater übernommen. Ein begründeter Verdacht liegt vor, wenn ein durchschnittlicher, verständiger und sorgfältiger Mitarbeiter der IT-Abteilung davon ausgehen kann, dass ein Cyber-Vorfall vorliegt.

Der Versicherer verzichtet im Falle der Feststellung, dass entgegen des begründeten Verdachts kein versicherter Versicherungsfall vorliegt, auf eine Rückforderung bereits geleisteter Versicherungsleistungen.

Es gilt ein Sublimit i.H.v. 25.000 EUR vereinbart.

d) Beweislasterleichterung
Der Eintritt eines Versicherten Schadenereignisses gilt bereits als erwiesen, wenn aufgrund objektiver Umstände nach der überwiegenden Wahrscheinlichkeit ein versichertes Schadenereignis gemäß Ziffer I. („Versicherungsschutz für Schadenersatzansprüche Dritter"), Ziffer II. („Versicherungsschutz bei Eigenschäden") und Ziffer III. („Datenschutzverfahren, Untersuchungen und Ermittlungen") für den Eintritt des Schadens ursächlich ist.

Die Anwendbarkeit der Beweislasterleichterung setzt voraus, dass nach Maßgabe dieser Bedingungen ein Cyber-Krisenberater durch Versicherte eingeschaltet wurde und die Versicherten ihre Mitwirkungs- und Anzeigeobliegenheiten erfüllt haben.

e) Leistung bei Eigenschäden
Es besteht Versicherungsschutz für die Übernahme der jeweils benannten Vermögensschäden bzw. der Übernahme der notwendigen und angemessenen Kosten.

f) Leistung bei Drittschäden
Für den Versicherungsschutz bei Drittschäden gilt:

i. Abwehr und Entschädigung
Es besteht Versicherungsschutz für die Prüfung der Haftpflichtfrage, die Abwehr von unbegründeten Schadenersatzansprüchen und die Freistellung von Versicherten bei begründeten Schadenersatzansprüchen.

Begründet sind Schadenersatzansprüche, wenn ein Versicherter aufgrund rechtskräftigen Urteils, Anerkenntnisse oder Vergleichs zur Entschädigung verpflichtet und der Versicherer hierdurch gebunden ist.

ii. Anerkenntnis/ Vergleich
Anerkenntnisse und Vergleiche, die von Versicherten ohne die Zustimmung des Versicherers abgegeben oder geschlossen wurden, binden den Versicherer nur, wenn und soweit der Anspruch auch ohne Anerkenntnis oder Vergleich bestehen würde.

iii. Freistellung von Ansprüchen
Ist die Schadenersatzverpflichtung der Versicherungsnehmerin mit bindender Wirkung für den Versicherer festgestellt, hat der Versicherer die Versicherungsnehmerin innerhalb von zwei Wochen vom Anspruch des Dritten freizustellen.

iv. Schadenregulierungsvollmacht
Der Versicherer ist bevollmächtigt, alle ihm zur Abwicklung des Schadens oder Abwehr der Schadenersatzansprüche gegen Versicherte zweckmäßig erscheinenden Erklärungen im Namen der Versicherten abzugeben. Die Versicherungsnehmerin bestätigt, dass der Versicherer auch für andere Versicherte bevollmächtigt ist.

v. Prozessführung
Wenn es zu einem Rechtsstreit über Schadenersatzansprüche gegen einen Versicherten kommt, ist der Versicherer zur Prozessführung berechtigt, aber nicht verpflichtet. Übernimmt der Versicherer die Prozessführung, trägt der Versicherer die Kosten und führt den Rechtsstreit im Namen des Versicherten.

Übernimmt der Versicherer die Prozessführung nicht, ersetzt er den Versicherten dennoch die Kosten des Rechtsstreits im Umfang gemäß der folgenden Ziffer vi.

Bei einem Rechtsstreit in den USA, US-Territorien oder Kanada oder nach deren Recht sind die Versicherten abweichend von oben genannter Regelung verpflichtet, den Rechtsstreit im eigenen Namen zu führen und sich gegen den Anspruch zu verteidigen. Dem Versicherer steht jedoch das Recht zu, an dem Prozess beteiligt zu werden oder gegebenenfalls die vollständige Prozessführung zu übernehmen.

vi. Rechtsanwaltswahl und Verfahrenskosten
Der Versicherer übernimmt die gebührenordnungsmäßigen Kosten nach dem Rechtsanwaltsvergütungsgesetz, dem Justizvergütungs- und Entschädigungsgesetz oder der entsprechenden ausländischen Rechtsordnungen. Je nach Schwierigkeit und Bedeutung des Sachverhaltes werden auch höhere Kosten im Rahmen von Honorarvereinbarungen übernommen, sofern diese angemessen sind und der Versicherer der Honorarvereinbarung zugestimmt hat. Die Wahl des Rechtsanwaltes wird den Versicherten überlassen, wobei ein Widerspruchsrecht aus sachlichem Grund für den Versicherer besteht.

Der Versicherer übernimmt auch die tatsächlich anfallenden gerichtlichen Verfahrenskosten inklusive der Entschädigung für Zeugen sowie die Entschädigungen und eventuell zu leistende Vorschüsse für gerichtlich bestellte Sachverständige oder Parteisachverständige.

g) Umstandsmeldung
Bei Drittschäden gemäß Ziffer I. „Versicherungsschutz für Schadenersatzansprüche Dritter“, Ziffer III. „Datenschutzverfahren, Untersuchungen und Ermittlungen“ und Ziffer. IV. „Entschädigungen mit Strafcharakter, Bußgelder, und PCI-Vertragsstrafen“ können Versicherte während der Vertragslaufzeit dem Versicherer Umstände melden, wenn eine Inanspruchnahme oder die Einleitung eines Versicherten Datenschutzverfahrens, Untersuchung oder Ermittlung gegen Versicherte hinreichend wahrscheinlich ist. Tritt aufgrund der gemeldeten Umstände ein Versicherungsfall ein, gilt dieser bereits zum Zeitpunkt der Umstandsmeldung als eingetreten. Es gelten die Bestimmungen zu Obliegenheiten und Obliegenheitsverletzungen gemäß Ziffer X. 12. d) und e) entsprechend.

4. Entschädigungsgrenzen
a) Versicherungssumme
Die vereinbarte Versicherungssumme ist die Höchstgrenze der vom Versicherer innerhalb einer Versicherungsperiode zu erbringenden Leistungen unter diesem Cyber-Versicherungsvertrag für jeden einzelnen Versicherungsfall und für alle Versicherungsfälle innerhalb der Versicherungsperiode zusammen.

Sämtliche Leistungen des Versicherers im Rahmen dieses Versicherungsvertrages werden auf die Versicherungssumme angerechnet. Das gilt insbesondere auch für Abwehrkosten im Rahmen von Ziffer I. „Versicherungsschutz für Schadenersatzansprüche Dritter“.

Die vereinbarte Versicherungssumme ist je Versicherungsjahr 1-fach maximiert.

b) Sublimite
Sublimite sind im Versicherungsschein geregelt und, sofern im Versicherungsschein nicht explizit etwas Anderes vereinbart wurde, sind die Sublimite die Höchstgrenze der zu erbringenden Leistung des Versicherers für den entsprechenden Versicherungsgegenstand.

Sublimite werden auf die Versicherungssumme angerechnet und verringern die für die laufende Versicherungsperiode zur Verfügung stehende Versicherungssumme um die Höhe der Auszahlung.

c) Selbstbehalt
Die Versicherungsnehmerin beteiligt sich bei jedem Versicherungsfall mit dem im Versicherungsschein festgelegten Betrag (Selbstbehalt), sofern nichts Anderes vereinbart ist.

Sind in einem Versicherungsfall mehrere Versicherungsgegenstände betroffen, findet der Selbstbehalt nur einmal Anwendung. Bei unterschiedlichen Selbstbehalten findet der höchste Selbstbehalt Anwendung.

5. Serienschaden
Mehrere während der Wirksamkeit des Cyber-Versicherungsvertrages eintretende Versicherungsfälle, die

- auf derselben Ursache beruhen, oder
- auf gleichen Ursachen beruhen, die in einem inneren, insbesondere sachlichen und zeitlichen Zusammenhang zueinanderstehen, oder
- aus der Erbringung von Dienstleistungen oder der Herstellung von Produkten mit gleichen Mängeln entstehen,

gelten unabhängig vom Zeitpunkt ihres Eintritts als ein Versicherungsfall und in dem Zeitpunkt eingetreten, in dem der erste Versicherungsfall eingetreten ist.

Der vereinbarte Selbstbehalt findet entsprechend Ziffer X. 5. d) nur einmal Anwendung.

6. Keine Schadenfallkündigung
Der Versicherer verzichtet abweichend von § 111 VVG nach Eintritt eines Versicherungsfalles auf das Recht, den Versicherungsvertrag aus diesem Grund zu kündigen.

7. Vorrangige Versicherung

Ist ein Versicherungsfall auch unter einem anderen Versicherungsvertrag versichert, so geht der vorliegende Cyber-Versicherungsvertrag als der speziellere Vertrag vor.

Dies gilt jedoch nicht, wenn es sich bei dem anderen Versicherungsvertrag ebenfalls um eine Cyber-Versicherung handelt; es kommt hierbei nicht auf die formale Bezeichnung, sondern auf die versicherten Leistungen im Vergleich zu dem vorliegenden Vertrag an. In diesem Fall steht der vorliegende Cyber-Versicherungsvertrag erst im Anschluss an die Versicherungssumme des anderen Versicherungsvertrages zur Verfügung (Summenausschöpfungsdeckung; „DIL-Deckung"). Im Übrigen besteht ergänzender Versicherungsschutz zu den Leistungen aus dem anderen Versicherungsvertrag, soweit der Versicherungsschutz unter dem vorliegenden Cyber-Versicherungsvertrag weiter ist als unter dem einschlägigen Versicherungsvertrag (Konditionendifferenzdeckung; „DIC-Deckung").

Enthält der anderweitig bestehende Versicherungsvertrag eine hiermit vergleichbare Regelung, so geht der Versicherungsvertrag vor, der zeitlich früher abgeschlossen wurde.

8. Kumulklausel

Ist der Versicherungsfall unter mehreren Versicherungsverträgen der W. R. Berkley Europe AG gedeckt, so ist die maximale Leistungspflicht der W. R. Berkley Gruppe gegenüber den Versicherten auf insgesamt 25 MEUR je Versicherungsfall und je Versicherungsperiode begrenzt. Die Versicherungssummen werden nicht kumuliert. In einem Kumulfall kommt ausschließlich der höchste anwendbare Selbstbehalt zur Anwendung. Die Regelung zum Selbstbehalt im Rahmen der Betriebsunterbrechung aus diesem Cyber-Versicherungsvertrag gemäß Ziffer II. 3. b) v. bleibt unberührt.

9. Sanktionen und Embargos

Unter diesem Cyber-Versicherungsvertrag besteht kein Versicherungsschutz, sofern die Bereitstellung von Versicherungsschutz gegen auf den Versicherer oder dessen oberste Muttergesellschaft direkt oder indirekt anwendbare Wirtschafts- oder Handelssanktionsgesetze oder -verordnungen, Finanzsanktionen oder Embargos verstoßen würde.

10. Vertragsänderungen

Vertragsänderungen und andere Anpassungen dieses Versicherungsvertrags sind nur wirksam, wenn diese vom Versicherer durch Nachtrag zu diesem Versicherungsvertrag dokumentiert werden.

11. Anzeigen/ Willenserklärungen/ Obliegenheiten

a) Textform

Für den Versicherer bestimmte Anzeigen, Erklärungen und Mitteilungen sind in Schrift- (§ 126 BGB) oder Textform (§ 126 b BGB) abzugeben und an die Hauptverwaltung des Versicherers zu richten:
W. R. Berkley Europe AG
Christophstraße 19
50670 Köln
E-Mail: **wrbvd_cyber@wrberkley.com**

b) Maklerklausel

Im Falle der Einschaltung eines Versicherungsmaklers, bzw. Q Versicherungsmakler GmbH ist dieser berechtigt, Anzeigen und Willenserklärungen der Versicherungsnehmerin entgegenzunehmen, und verpflichtet, diese unverzüglich an den Versicherer weiterzuleiten.

Des Weiteren ist der Versicherungsmakler, bzw. Q Versicherungsmakler GmbH berechtigt, alle Anzeigen und Willenserklärungen des Versicherers mit unmittelbarer Wirkung für und gegen die Versicherungsnehmerin entgegenzunehmen.

c) Gefahrerhöhung während der laufenden Versicherungsperiode

Als Gefahrerhöhung unter diesem Cyber-Versicherungsvertrag gelten ausschließlich nachfolgend genannte während der Vertragslaufzeit eintretende Umstände. Im Fall einer Gefahrerhöhung hat die Versicherungsnehmerin dem Versicherer die Gefahrerhöhung unverzüglich und in Textform anzuzeigen. Tritt ein anzeigepflichtiger Umstand ein, hat der Versicherer nach Erhalt der Anzeige das Recht, die Versicherungsbedingungen und/ oder Versicherungsprämie anzupassen. Wird nach Anzeige der Gefahrerhöhung innerhalb von zwei (2) Monaten keine Einigung über die neuen Konditionen erzielt, entfällt der Versicherungsschutz für die Versicherungsfälle, die im Zusammenhang mit der angezeigten Gefahrerhöhung stehen, rückwirkend nach Maßgabe der folgenden Regelungen:

- Neubeherrschung der Versicherungsnehmerin
- Verschmelzung der Versicherungsnehmerin
- Verschmelzung auf die Versicherungsnehmerin
- Änderung der Hauptgeschäftstätigkeit der Versicherungsnehmerin
- Insolvenz der Versicherungsnehmerin
- Neue Tochtergesellschaften, die nicht die Voraussetzungen für den automatischen Einschluss gemäß VIII. 3 b) i. erfüllen.

Die Rechtsfolgen einer Gefahrerhöhung bestimmen sich nach den §§ 23 ff. VVG.

d) Obliegenheiten im Versicherungsfall

Für den Fall, dass ein Versicherungsfall eintritt, nehmen die Versicherten unverzüglich Kontakt zum Cyber-Krisenberater auf. Die Versicherten haben dem Versicherer folgende Umstände im Versicherungsfall unverzüglich in Textform anzuzeigen und folgende Obliegenheiten zu erfüllen:

- Anzeige der Geltendmachung eines gegen sie gerichteten Anspruchs;
- Anzeige von eröffneten (internen oder behördlichen) Ermittlungs-/Untersuchungsverfahren, Mahnbescheide, Strafbefehle, Streitverkündungen, einstweilige Verfügungen und Anträge auf Prozesskostenhilfe durch den Anspruchsteller; Weisungsrecht des Versicherers und Mitwirkungspflicht der Versicherten Die Versicherten sind verpflichtet, den Weisungen des Versicherers zu folgen, sofern von ihnen nichts Unbilliges verlangt wird. Sie sind ferner verpflichtet, den Versicherungsfall nach Möglichkeit zu verhindern bzw. den Schaden zu mindern und alles zu unternehmen, was der Aufklärung des Versicherungsfalles dient, insbesondere dem Versicherer alle Auskünfte zu erteilen, die für die Feststellung des Versicherungsfalls oder des Umfangs der Leistungspflicht des Versicherers erforderlich sind. Der Versicherer wird bei der Prüfung und Abwicklung des Versicherungsfalls, insbesondere der Schadenermittlung und -regulierung sowie der Abwehr von Schadensersatzansprüchen Dritter, von den Versicherten unterstützt. Dies beinhaltet eine ausführliche und wahrheitsgemäße Berichterstattung aller den Versicherungsfall und Schadenfolgen betreffenden Tatsachen sowie eine unverzügliche Überlassung aller vom Versicherer angeforderten Unterlagen, die für eine Beurteilung des Versicherungsfalles notwendig sind; dies gilt auch für die Beschaffung von Unterlagen, soweit den Versicherten insoweit nichts Unbilliges zugemutet wird.
- Wahrung von Regressansprüchen: Hat der Versicherer Versicherungsleistungen erbracht, gehen die Regressansprüche von Versicherten auf den Versicherer über. Die Übertragung kann nicht nachteilig für die Versicherten ausgelegt werden. Zur Sicherung von Regeressansprüchen haben die Versicherten hierzu bestehende Rechte unter Wahrung der geltenden Form- und Fristvorschriften zu wahren und den Versicherer, soweit erforderlich, bei deren Durchsetzung zu unterstützen. Der Versicherer ist nicht zur Leistung verpflichtet, wenn ein Versicherter hiergegen vorsätzlich verstößt, sodass in der Folge kein Regress gegenüber Dritten möglich ist. Bei einer grob fahrlässigen Verletzung der Obliegenheit seitens der Versicherten kann der Versicherer seine Leistung in einem Verhältnis kürzen, welches die Schwere des Verschuldens widerspiegelt. Die Versicherten tragen die Beweislast, dass keine grobe Fahrlässigkeit vorliegt.

- Abtretungsverbot: Der Freistellungsanspruch darf vor seiner endgültigen Feststellung ohne Zustimmung des Versicherers weder abgetreten noch verpfändet werden. Eine Abtretung an den geschädigten Dritten ist jedoch zulässig.
- Verfahrensführung: Bei einem (außer-)gerichtlichen (Rechts-)Streit oder Verfahren hinsichtlich eines Schadensersatzanspruchs Dritter überlässt der Versicherte nach Maßgabe der Anforderungen des Versicherers die Verfahrensführung dem Versicherer.
- Rechtsbehelfe: Die Versicherten werden gegen Mahnbescheide, Urteile oder Verfügungen von Verwaltungsbehörden auf Schadenersatz fristgerecht die erforderlichen Rechtsbehelfe einlegen, sofern der Versicherer keine abweichende Weisung erteilt.
- Regulierungsvollmacht: Der Versicherer ist bevollmächtigt, alle ihm zweckmäßig erscheinenden gerichtlichen bzw. außergerichtlichen Erklärungen im Namen der Versicherten abzugeben, die dazu dienen, einen Schadensersatzanspruch Dritter abzuwehren oder beizulegen.
- Im Falle einer Cyber-Erpressung gilt zusätzlich, dass die Versicherten: Alle angemessenen Maßnahmen ergreifen, um festzustellen, dass es sich hierbei um eine ernsthafte Drohung handelt. In Abstimmung mit dem Cyber-Krisenberater die Cyber-Erpressung unverzüglich bei der zuständigen Polizei und gegebenenfalls anderen zuständigen Behörden anzeigen; außerhalb Europas gilt dies nur, sofern dies nach Abstimmung mit dem Cyber-Krisenberater notwendig und sinnvoll ist. Vor Zahlung eines Cyber-Erpressungsgeldes die Empfehlung des Cyber-Krisenberaters einholen und sich auf dieser Grundlage vor Bezahlung des Cyber-Erpressungsgeldes mit dem Versicherer abstimmen. Die Wiedererlangung von Cyber-Erpressungsgeld ist dem Versicherer unverzüglich anzuzeigen und dieses dem Versicherer zurückzuerstatten.
- Schadenmeldung: Sämtliche Cyber-Umstandsmeldungen und Cyber-Schadenmeldungen sind dem Versicherer unverzüglich an folgende E-Mail-Adresse zu melden:

wrbvd_schaden_cyber@wrberkley.com

e) Obliegenheitsverletzung

Wird eine Obliegenheit verletzt, die gegenüber dem Versicherer vor Eintritt des Versicherungsfalles zu erfüllen ist, so kann der Versicherer den Vertrag innerhalb eines Monats nachdem er von der Verletzung Kenntnis erlangt hat, fristlos kündigen. Der Versicherer hat jedoch kein Recht zur Kündigung, wenn die Versicherungsnehmerin nachweist, dass die Verletzung der Obliegenheit weder auf Vorsatz noch auf grober Fahrlässigkeit beruht.

Wird eine dem Versicherer gegenüber zu erfüllende Obliegenheit vorsätzlich verletzt, wird der Versicherer leistungsfrei. Bei grob fahrlässiger Verletzung der Obliegenheit ist der Versicherer berechtigt, seine Leistung in einem der Schwere des Verschuldens der Versicherungsnehmerin bzw. der Versicherten entsprechenden Verhältnis zu kürzen. Die Beweislast für das Nichtvorliegen grober Fahrlässigkeit trägt die Versicherungsnehmerin bzw. tragen die Versicherten.

Der Versicherer bleibt jedoch zur Leistung verpflichtet, soweit die Versicherungsnehmerin nachweist bzw. die Versicherten nachweisen, dass die Verletzung der Obliegenheit weder für den Eintritt oder die Feststellung des Versicherungsfalles noch für die Feststellung oder den Umfang der dem Versicherer obliegenden Leistung ursächlich ist. Dies gilt nicht, wenn die Versicherungsnehmerin bzw. Versicherte die Obliegenheit arglistig verletzt hat.

12. Fremdwährung

Ist die Versicherungsleistung in einem Versicherungsfall nicht in EURO zu leisten, wird der am Tag der Auszahlung durch den Versicherer gültige Devisen-Referenzkurs der Europäischen Zentralbank zugrunde gelegt.

13. Gerichtsstand und Anwendbares Recht

Für Streitigkeiten aus oder im Zusammenhang mit diesem Cyber-Versicherungsvertrag sind ausschließlich deutsche Gerichte zuständig.

Der Cyber-Versicherungsvertrag unterliegt ausschließlich deutschem Recht. Es gelten insbesondere die Vorschriften des Versicherungsvertragsgesetzes (VVG), sofern durch diesen Cyber-Versicherungsvertrag nichts Anderes geregelt wird.

14. Beschwerden

Beschwerden können, außer an den Versicherer selbst, auch an die Bundesanstalt für Finanzdienstleistungsaufsicht, Graurheindorfer Straße 108 in 53117 Bonn, gerichtet werden.

***

Über W. R. Berkley Corporation

Die W. R. Berkley Corporation wurde 1967 gegründet und gehört zu den inhabergeführten „Fortune 500“ Unternehmen der USA. Mit 54 operativen Einheiten in über 15 Ländern und mit über 7.600 Mitarbeitenden handelt es sich um eine der großen Versicherungsgesellschaften weltweit.

Berkley Deutschland

Seit 2010 agieren wir in Deutschland und Österreich als etablierter Spezialversicherer für kleine und mittelständische Unternehmen insbesondere in den Sparten Financial Lines, Haftpflicht und Cyber. Für unsere Kunden entwickeln wir maßgeschneiderte Versicherungslösungen: professionell, effizient und bedarfsorientiert.

„Wir versichern nicht nur, wir übernehmen Verantwortung.“

Diesem Leitspruch folgend zählt für uns bei der Gestaltung von Versicherungsschutz jedes Detail, sowohl fachlich, als auch menschlich. Unsere Mitarbeitenden bringen eine Vielfalt an Fähigkeiten mit: hervorragende Fachkenntnis, große Erfahrung in der Einschätzung von Risiken sowie Freude an der kreativen Entwicklung individueller Versicherungslösungen und darüber hinausgehenden Serviceleistungen.

Warum Berkley der richtige Partner ist

Finanzielle Sicherheit

Sowohl von Standard & Poors‘s als auch von A.M. Best wird W. R. Berkley Corporation mit einem überdurchschnittlichen Rating eingestuft (A+).

Weltweit erfolgreich

Im Jahr 1967 gegründet, zählt W. R. Berkley Corporation weltweit 54 Unternehmen mit über 7.600 Mitarbeitenden in mehr als 15 Ländern.

Optimale Versicherungslösungen

Bei der Gestaltung von individuellen und zukunftsfähigen Versicherungslösungen zählt bei uns jedes Detail – fachlich und menschlich.

W. R. Berkley Europe AG
Niederlassung für Deutschland

Standort Köln
Christophstraße 19
50670 Köln

Standort München
Werner-Eckert-Straße 14
81829 München

Besuchen Sie unsere Website

Berkley
DEUTSCHLAND
a Berkley Company