Du bist nicht allein.
R+V Allgemeine Versicherung AG
Raiffeisenplatz 1
65189 Wiesbaden
www.ruv.de

R+V-WirtschaftsschutzPolice Risikofragebogen

Damit wir Ihnen ein Angebot zur R+V-WirtschaftsschutzPolice machen können, brauchen wir verschiedene Angaben von Ihnen.

A. Angaben zum Unternehmen/Versicherungsnehmer

Name/Firma _____

Ansprechpartner _____

Straße, Hausnummer _____

PLZ, Ort _____

Telefon _____

Telefax _____

E-Mail _____

Sie können der Nutzung Ihrer E-Mail-Adresse jederzeit widersprechen. Eine E-Mail an redaktion@ruv.de genügt.

Internetadresse _____

Betriebsbeschreibung _____

Nettoumsatz (letztes Geschäftsjahr) _____ EUR

Bitte geben Sie hier den Nettoumsatz des Versicherungsnehmers an, erst nachfolgend die seiner Tochterunternehmen. Unter Punkt C. ist der konsolidierte Nettoumsatz anzugeben.

Anzahl der Mitarbeiter _____ Agentur-Nr. _____

R+V-Kundennummer (falls vorhanden) _____

Mitzuversichernde rechtlich selbstständige Unternehmen, Betriebsstätten, Standorte im Inland.

1. Unternehmen Beteiligungsquote _____ %

Name/Firma _____

Straße, Hausnummer _____

PLZ, Ort _____

Betriebsbeschreibung _____

Nettoumsatz (letztes Geschäftsjahr) _____ EUR Anzahl der Mitarbeiter _____

2. Unternehmen Beteiligungsquote _____ %

Name/Firma _____

Straße, Hausnummer _____

PLZ, Ort _____

Betriebsbeschreibung _____

Nettoumsatz (letztes Geschäftsjahr) _____ EUR Anzahl der Mitarbeiter _____

Mitzuversichernde rechtliche selbständige Unternehmen, Betriebsstätten, Standorte im Ausland. (falls Sie weitere Standorte außerhalb der Bundesrepublik Deutschland unterhalten)

Unternehmen Beteiligungsquote _____ %

Name/Firma _____

Straße, Hausnummer _____

PLZ, Ort, Land _____

Betriebsbeschreibung _____

Nettoumsatz (letztes Geschäftsjahr) _____ EUR Anzahl der Mitarbeiter _____

Weitere mitzuversichernde Unternehmen im In- oder Ausland nennen Sie uns bitte auf einem separaten Blatt.

B. Verpflichtungen des Interessenten, Angaben zum Vorversicherungsverhältnis

1. Bestand bereits eine Versicherung gegen Cyber-Risiken? ☐ Nein ☐ Ja, bei _____

2. Bestand bereits eine Vertrauensschadenversicherung? ☐ Nein ☐ Ja, bei _____

3. Wenn Sie eine der ersten beiden Fragen (1. oder 2.) mit „Ja“ beantwortet haben:
   Wurde der Vertrag durch den Versicherer gekündigt? ☐ Nein ☐ Ja

4. Sind in den letzten fünf Jahren Schäden durch

   a. den Gebrauch von Informations- und Telekommunikationsgeräten entstanden? ☐ Nein ☐ Ja

   b. Wirtschaftskriminalität entstanden?
   Darunter fallen insbesondere Vermögensstraftaten durch Mitarbeiter oder Dritte, Geheimnisverrat oder wissentliche Pflichtverletzungen. ☐ Nein ☐ Ja

   Wenn Sie eine der beiden vorherigen Fragen (4. a. oder b.) mit „Ja“ beantwortet haben, geben Sie uns bitte die folgenden Informationen zu diesen Schäden:

Schaden	Schadenhöhe	Schadenursache/-verursacher	Schadenjahr
☐ Cyber ☐ VSV	EUR		
☐ Cyber ☐ VSV	EUR		
☐ Cyber ☐ VSV	EUR		

C. Produktions- und Lieferprogramm

Nettoumsatz (konsolidiert) des letzten Geschäftsjahrs _____ EUR

davon Online-Handel in % _____ %

Anteiliger Umsatz mit

- Produkten aus eigener Herstellung (Eigenprodukte) _____ EUR
- Handelsware _____ EUR
- Importierte Waren aus Nicht-EU-Ländern _____ EUR
- Sonstige Leistungen _____ EUR

Soweit vorhanden:

Umsatz mit IT-Dienstleistungen für Dritte (nicht Mitversicherte) _____ EUR

Welche IT-Dienstleistungen* werden für Dritte erbracht? _____

*Eventuell sind diese Tätigkeiten über die IT-Haftpflicht oder Betriebshaftpflichtversicherung versicherbar.

Werden Ihre Erzeugnisse durch Ihre Abnehmer weiterverarbeitet,
so dass durch Verbindung/Vermischung ein neues Produkt entsteht? ☐ Nein ☐ Ja

D. Gewünschte Versicherungssummen, Selbstbeteiligung, Zusatzbausteine

1. Cyber Versicherung

Versicherungssumme _____ EUR
(eigenständige Versicherungssumme)

Generelle Selbstbeteiligung pro Versicherungsfall _____ EUR
(ab 1 Mio. EUR VSU, mind. 5.000 EUR Selbstbeteiligung)

Gewünschte Zusatzbausteine

Aufwendungen vor Eintritt des Versicherungsfalls	☐ Nein	☐ Ja
Eigenschäden durch technische Hardwaredefekte	☐ Nein	☐ Ja
Betriebsunterbrechung in Folge nicht korrekter Daten	☐ Nein	☐ Ja
Betriebsunterbrechung in Folge nicht nutzbarer IT-Dienstleistungen	☐ Nein	☐ Ja
Betriebsunterbrechung nach einer Straftat beim IT-Dienstleister	☐ Nein	☐ Ja
Bring your own device (BYOD) - Mitversicherung privater Daten	☐ Nein	☐ Ja
Diebstahl von Vermögenswerten in Folge einer Informationssicherheits-verletzung (Cyber-Diebstahl)	☐ Nein	☐ Ja

2. Vertrauensschadenversicherung

Versicherungssumme _____ EUR
(eigenständige Versicherungssumme)

Generelle Selbstbeteiligung pro Versicherungsfall _____ EUR
Die Selbstbeteiligung für Schäden durch Dritte beträgt 10 %, mind. 5.000 EUR.

E. Fragen zur Cyber Versicherung

Fragen zu entgeltlich vereinbarten IT-Dienstleistungen (Cloud-Computing)

1. Nutzen Sie vertraglich vereinbarte sogenannte Infrastructure as a Service (IaaS) IT-Dienstleistungen?
IT-Dienstleister stellen vertraglich vereinbarte IT-Infrastruktur, insbesondere sogenannte Computer-, Speicher- und Netzwerkressourcen, bedarfsgerecht und mit nutzungsbasierter Bezahlung zur Verfügung. ☐ Nein ☐ Ja

Wenn ja, geben Sie bitte folgende Informationen an:

IT-Dienstleister	Beschreibung der IT-Dienstleistung – bezogene Leistungen und Umfang

2. Nutzen Sie vertraglich vereinbarte sogenannte Plattform as a Service (PaaS) IT-Dienstleistungen?
IT-Dienstleister stellen vertraglich vereinbarte Hardware und Anwendungssoftware-plattformen, z. B. Datenbanksysteme, bedarfsgerecht und mit nutzungsbasierter Bezahlung zur Verfügung. ☐ Nein ☐ Ja

Wenn ja, geben Sie bitte folgende Informationen an:

IT-Dienstleister	Beschreibung der IT-Dienstleistung – bezogene Leistungen und Umfang

3. Nutzen Sie vertraglich vereinbarte sogenannte Software as a Service (SaaS) IT-Dienstleistungen?
IT-Dienstleister stellen vertraglich vereinbarte Software und Anwendungen, z. B. Office365, bedarfsgerecht und mit nutzungsbasierter Bezahlung zur Verfügung. ☐ Nein ☐ Ja

Wenn ja, geben Sie bitte folgende Informationen an:

IT-Dienstleister	Beschreibung der IT-Dienstleistung – bezogene Leistungen und Umfang

Fragen zu IT Governance, Risk und Compliance (GRC)

4. **Ist ein Information Security Management System (Managementsystem für Informationssicherheit) etabliert?**
   Wenn ja, fügen Sie bitte die entsprechende Leitlinie zur Informationssicherheit und – sofern zertifiziert – die Zertifizierung bei.
   ☐ Nein ☐ Ja

Fragen zum Schutz von Benutzerkonten

5. **Setzen Sie nicht personalisierte Benutzerkonten ein (Shared User Accounts)?** Nicht personalisierte Benutzerkonten sind Konten, die keine technischen Konten sind oder für Services genutzt werden und nicht einer einzelnen natürlichen Person eindeutig zugewiesen worden sind. Z. B. nutzt eine Gruppe von Personen dasselbe Benutzerkonto?
   ☐ Nein ☐ Ja

6. **Ist eine Passwortrichtlinie vorhanden, mit der Sie eine ausreichende Passwortkomplexität vorgeben?**
   Die Passwortkomplexität ist abhängig von der Implementierung (z. B. nach fünf Fehlversuchen wird das Konto gesperrt) und von der technischen Entwicklung. Hinweise, was zum aktuellen Stand der Technik eine ausreichende Passwortkomplexität ist, finden Sie u. a. auf den Seiten des Bundesamt für Sicherheit in der Informationstechnik (BSI).
   ☐ Nein ☐ Ja

7. **Stellen Sie mit technischen Mitteln die Einhaltung der Passwortrichtlinie sicher?**
   Beispielsweise im Windows-Umfeld, Sicherstellungen mit entsprechenden Richtlinien (Policy).
   ☐ Nein ☐ Ja

8. **Haben Sie vorgegeben, dass administrative Benutzerkonten nur für administrative Tätigkeiten eingesetzt werden dürfen?**
   Für die normale tägliche Arbeit dürfen keine Administratorenrechte verwendet werden.
   ☐ Nein ☐ Ja

Fragen zum Schutz der Netzwerkinfrastruktur

9. **Gibt es ein Sicherheitskonzept, das aufzeigt, wie Sie das bzw. die Unternehmensnetzwerk(e) absichern?**
   Im Rahmen eines Sicherheitskonzeptes wird aufgezeigt, wie mit Gefährdungen umgegangen werden soll. Das Sicherheitskonzept operationalisiert Sicherheitsvorgaben und zeigt auf, wie diese technisch umgesetzt und auf einander abgestimmt werden sollen.
   ☐ Nein ☐ Ja

10. **Ist Ihr internes Netzwerk mit einer externen Firewall gesichert?**
    Eine externe Firewall kontrolliert die Verbindung zwischen zwei Netzen und dient dazu, den Netzwerkzugriff zu beschränken.
    ☐ Nein ☐ Ja

11. **Sind Zugriffe auf das interne Netzwerk aus dem Internet heraus nur mit Hilfe verschlüsselter Verfahren möglich?**
    Um sicherzustellen, dass die Kommunikation nicht unbefugt mitgelesen, unbefugt kopiert bzw. verfälscht wird, müssen weitere Maßnahmen eingesetzt werden, z. B. verschiedene Protokolle (u. a. IPSec, SSL/TLS) oder Softwarelösungen (u. a. VPN).
    ☐ Nein ☐ Ja

Fragen zum IT-Betrieb

12. **Haben Sie ein Patch-Management-Verfahren, das eine zeitnahe Installation von Sicherheitspatches sicherstellt?**
    Regelmäßig werden neue Schwachstellen in IT-Systemen gefunden, wodurch diese angreifbar werden. Zur Schließung dieser Schwachstellen werden Sicherheitspatches bereitgestellt.
    ☐ Nein ☐ Ja

13. Haben Sie ein Verfahren zum Umgang mit IT-Systemen, welche bekannte Schwachstellen haben, die aus technischen Gründen nicht gepatcht werden können, im Gebrauch, z. B. IT-Systeme im industriellen Einsatz, IT-Systeme zur Steuerung von Geräten und Maschinen etc.?
IT-Systeme mit bekannten Schwachstellen müssen durch ergänzende Maßnahmen geschützt werden, wenn die Schwachstelle nicht mit einem Sicherheitspatch geschlossen werden kann.

Wenn ja, geben Sie bitte folgende Informationen an: ☐ Nein ☐ Ja

IT-Systeme	Maßnahmen

Fragen zur Fähigkeit Ihres Unternehmens, sich nach einem Cyber-Vorfall wieder erholen zu können

14. Gibt es eine abgestimmte und implementierte IT-Notfallplanung, so dass der Betrieb der kritischen bzw. zeitkritischen IT-Systeme den geschäftlichen Anforderungen entsprechend wiederhergestellt werden kann?
Ausfälle, Probleme, Störungen oder Notfälle sowie Cyber-Angriffe gehören zum IT-Alltag. Es müssen Vorbereitungen getroffen werden, damit IT-Systeme und Daten entsprechend des geschäftlichen Bedarfs wiederhergestellt werden können. ☐ Nein ☐ Ja

15. Beim Einsatz/Nutzung eines Microsoft Windows Domain Controllers: Gibt es eine abgestimmte und implementierte IT-Notfallplanung, so dass die Wiederherstellung der Windows Domäne sowie aller in der Domäne eingebundenen Systeme, Clients und Dienste den geschäftlichen Anforderungen entsprechend sichergestellt wird?
Wie lange wird nach Ihrer Notfall-Planung die Wiederherstellung der Windows Domäne sowie aller in der Domäne eingebundenen Systeme, Clients und Dienste dauern?

Zeitangabe in Tagen
_____ mindestens
_____ maximal
_____ erwartet

16. Beim Einsatz/Nutzung eines Typ-1-Hypervisor (z. B. VMware ESX/ESXi, XEN, Hyper-V): Gibt es eine abgestimmte und implementierte IT-Notfallplanung, so dass die Wiederherstellung der virtuellen Maschinen den geschäftlichen Anforderungen entsprechend sichergestellt wird?
Wie lange wird nach Ihrer Notfall-Planung die Wiederherstellung der virtuellen Maschinen dauern?

Zeitangabe in Tagen
_____ mindestens
_____ maximal
_____ erwartet

17. Werden regelmäßig Tests zur Wiederherstellung von IT-Systemen (z. B. Betriebssysteme, Warenwirtschaftssysteme, Datenbanken etc.) durchgeführt?
Vorgehen und Verfahren müssen getestet werden, so dass Sie sicher sein können, dass diese im Notfall auch funktionieren werden. ☐ Nein ☐ Ja

18. Werden regelmäßig Tests zur Wiederherstellung von Datenbeständen und deren Nutzbarkeit durchgeführt?
Vorgehen und Verfahren müssen getestet werden, so dass Sie sicher sein können, dass diese im Notfall auch funktionieren werden. ☐ Nein ☐ Ja

19. Haben Sie sichergestellt, dass die Datensicherung nicht durch dieselbe Ursache manipuliert, beschädigt oder unbrauchbar gemacht werden kann, wie die Originaldaten?
Datensicherungen müssen vor Manipulationen oder dem Unbrauchbarmachen geschützt werden. Hierzu müssen entsprechende Maßnahmen getroffen werden, weil sonst die Gefahr besteht, dass Datensicherungen durch dieselbe Ursache unbrauchbar oder manipuliert werden und nicht mehr für die Wiederherstellung verwendet werden können. ☐ Nein ☐ Ja

Fragen zum Schadenpotential, wenn IT-Systeme oder kritische Daten nicht verfügbar sind

20. Bei Vorliegen eines vollständigen IT-Ausfalls (z. B. der Windows Domain Controller, virtuellen Maschinen im Hypervisor, Daten des Warenwirtschafts-systems), wodurch IT-Systeme und Daten nicht zur Verfügung stehen:

a. Wieviel Zeit haben Sie für die Wiederherstellung der IT, bevor die Geschäftsauswirkungen kritisch werden?

Zeitangabe in Tagen

_____ mindestens
_____ maximal
_____ erwartet

b. Bezogen auf das gesamte Geschäftsjahr: Können Sie die durch die Betriebsunterbrechung verursachten Rückstände nacharbeiten?
Wenn nein, was und warum nicht? Bitte erläutern Sie das auf einem separaten Blatt.

☐ Nein ☐ Ja

F. Zusatzfragen zur Cyber Versicherung für Interessenten
- **mit einem Jahresnettoumsatz > 100 Mio. EUR oder**
- **gewünschter Versicherungssumme > 1 Mio. EUR**

Fragen zur IT-Governance, Risk und Compliance (GRC)

1. Haben Sie einen Informationssicherheitsbeauftragten (ISB)?
IT-Sicherheit ist sehr komplex und facettenreich und bedarf entsprechender Spezialisten. Zur konsequenten Umsetzung von Sicherheitsmaßnahmen werden diese durch den ISB abgestimmt und gesteuert.

☐ Nein ☐ Ja

2. Quantifizieren Sie Risiken, die mit der Nutzung Ihrer Daten, IT-Systeme oder IT-Services einhergehen?
Pflicht für Unternehmen, die nach § 91 Abs. 2 AktG ein Risikofrüherkennungssystem betreiben müssen. Prüfungsgrundlage ist u. a. der Standard IDW PS 340.

☐ Nein ☐ Ja

3. Haben Sie ein IT-Sicherheitskonzept, das umgesetzt wird?
Einzelne Sicherheitsmaßnahmen müssen aufeinander abgestimmt sein, so dass die gewünschte Schutzwirkung erreicht wird.

☐ Nein ☐ Ja

Fragen zum Schutz von Benutzerkonten

4. Dokumentieren Sie, wie IT-Berechtigungen vergeben, verändert, entzogen und gelöscht werden?
Ohne Dokumentation ist schwer nachvollziehbar, wer genau welche IT-Berechtigungen wann und für was erhalten hat.

☐ Nein ☐ Ja

5. Sofern Sie über das Internet bereitgestellte Services (z. B. Microsoft Azure) nutzen: Sind die Konten durch eine Zwei-Faktor-Authentifizierung gesichert (2FA)?
Die reine Absicherung von Konten mit Hilfe von Benutzername und Passwort ist bei Anmeldeverfahren, die über das Internet stattfinden, problematisch. Aktuelle Angriffs-techniken müssen mit weiterführenden Sicherheitsmaßnahmen ergänzt werden.

☐ Nein ☐ Ja

6. Ist ein Sicherheitskonzept implementiert, das Angriffe mit Hilfe gestohlener oder extrahierter Anmeldeinformationen (Credential Dumping) berücksichtigt?
Standardangriffe nutzen aus Computer- und Programmspeichern (Cache) ausgelesene Anmelde- und Zugangsinformationen – siehe z. B. Technik T1003 des att&ck Rahmenwerks, att&ck T1003.

☐ Nein ☐ Ja

Fragen zum Schutz der Netzwerkinfrastruktur

7. Ist sichergestellt, dass IT-Geräte (z. B. Computer, Laptops, Mobiltelefone, Router etc.) nicht ohne Freigabe durch den zuständigen Netzwerkadministrator mit dem internen Netzwerk verbunden werden können?
Es kann nicht verhindert werden, dass Systeme ungefragt und unberechtigt mit dem internen Netzwerk physisch verbunden werden, aber sie dürfen keinen Zugang zum Netzwerk erhalten.

☐ Nein ☐ Ja

Fragen zum IT-Betrieb

8. **Gibt es verbindliche Verfahren, um Hardware und Software in Betrieb zu nehmen und sicher zu konfigurieren?**
   Auswahl, Abstimmung, Inbetriebnahme und Konfiguration sind komplexe Abläufe, die abgestimmt sein müssen, ansonsten können schwerwiegende Fehler und Sicherheitslücken entstehen. ☐ Nein ☐ Ja

9. **Gibt es verbindliche Verfahren, die sicherstellen, dass alle für den IT-Betrieb notwendigen Komponenten (Hardware und Software) sicher konfiguriert sind?**
   Entsprechend des Einsatzzwecks, der Art und Weise, wie und in welchem Kontext der Einsatz stattfindet, muss eine entsprechende Konfiguration stattfinden. Grundlage sind die Best-Practice-Empfehlungen der Hersteller. ☐ Nein ☐ Ja

Fragen zur Detektion und Reaktion auf sicherheitsrelevante Vorfälle

10. **Gibt es ein Konzept, aus dem hervorgeht, welche Daten zu Sicherheitszwecken wo und in welcher Form gesammelt und gespeichert werden?**
    Es muss festgelegt werden, was festgestellt werden soll, um zu definieren, wie und in welcher Form die dafür notwendigen Daten beschafft bzw. generiert werden. ☐ Nein ☐ Ja

11. **Ist eine technische Lösung implementiert, mit der die sicherheitsrelevanten Daten gespeichert und ausgewertet werden können?**
    Sicherheitsrelevante Informationen von z. B. Servern, Clients, Routern, Firewalls etc. müssen vor Manipulationen und Löschung geschützt werden. Damit Sie auch zielführend analysiert werden können, müssen sie auch zusammengeführt werden. Beispiel für eine technische Lösung ist Splunk. ☐ Nein ☐ Ja

12. **Ist ein Security Information and Event Management System (SIEM) im Einsatz?** ☐ Nein ☐ Ja

13. **Werden IT-Systeme kontinuierlich mit technischen Mitteln, z. B. einem Schwachstellenscanner, gezielt auf bekannten Schwachstellen geprüft?**
    Nicht alle Schwachstellen können mit Hilfe automatisch aufgespielter Sicherheitspatches geschlossen werden. In vielen Situationen müssen die IT-Systeme einzeln auf das Vorhandensein bekannter Schwachstellen geprüft werden. ☐ Nein ☐ Ja

14. **Werden sicherheitsrelevante Daten systematisch ausgewertet und analysiert?** ☐ Nein ☐ Ja

15. **Werden nicht erfolgreiche Anmeldeversuche an Konten bzw. IT-Systemen erfasst?**
    Fehlgeschlagene Anmeldungen können auf Fehler eines berechtigten Benutzers zurückgeführt werden. Sie können aber auch ein Zeichen dafür sein, dass Unberechtigte sich Zugang zu Konten bzw. IT-Systemen verschaffen wollen, z. B. mit Hilfe eines Brute-Force-Angriffs. ☐ Nein ☐ Ja

16. **Gibt es Vorgaben, wie zeitnah auf nicht erfolgreiche Anmeldeversuche an Konten bzw. IT-Systemen zu reagieren ist?**
    Wenn der Verdacht besteht, dass Unberechtigte versuchen, sich Zugang zu Konten oder IT-Systemen zu verschaffen, muss diesem Verdacht gezielt nachgegangen werden. Idealerweise wird der Versuch eines unberechtigten Zugangs unterbunden. ☐ Nein ☐ Ja

G. Fragen zur Vertrauensschadenversicherung

1. **Verfügt Ihr Unternehmen über eine Revisionsabteilung?** ☐ Nein ☐ Ja

2. **Führt die Revisionsabteilung in jedem Ihrer Betriebe mindestens einmal jährlich eine komplette Betriebsprüfung durch?** ☐ Nein ☐ Ja

3. **Stehen die Kontrollsysteme im Einklang mit allen Empfehlungen der externen Revision?** ☐ Nein ☐ Ja

4. **Wer führt bei Ihnen interne Revisionen durch?** _____

5. Gab es im letzten Wirtschaftsprüfungs-Abschlussbericht Beanstandungen zu internen Kontrollen? ☐ Nein ☐ Ja

Wenn ja, geben Sie bitte an, was genau beanstandet wurde:

_____

_____

6. Wurden nach der letzten Prüfung alle Empfehlungen des Wirtschaftsprüfers zu internen Kontrollen befolgt? ☐ Nein ☐ Ja

Wenn nein, nennen Sie bitte die Gründe:

_____

_____

7. Wann erfolgen bei Ihnen Inventuren? ☐ monatlich ☐ halbjährlich ☐ vierteljährlich ☐ jährlich

8. Welche Maßnahmen nutzen Sie, um Schäden zu verhüten oder zu entdecken?

Vier-Augen-Prinzip	☐ Nein ☐ Ja
Trennung von Kasse und Buchhaltung	☐ Nein ☐ Ja
Laufende Budgetkontrollen	☐ Nein ☐ Ja
Laufende Kassen- und Bücherrevisionen	☐ Nein ☐ Ja
Der Warenbestand wird regelmäßig von anderen als den dafür verantwortlichen Personen geprüft.	☐ Nein ☐ Ja

9. Können Mitarbeiter mit alleiniger Unterschrift…

Schecks > 10.000 EUR zeichnen?	☐ Nein ☐ Ja
Überweisungen/Anweisungen tätigen?	☐ Nein ☐ Ja
neue Bankkonten eröffnen?	☐ Nein ☐ Ja
Kontoauszüge entgegennehmen oder verschicken?	☐ Nein ☐ Ja
Bargeldauszahlungen vornehmen?	☐ Nein ☐ Ja
Waren zurückgeben oder zurücknehmen?	☐ Nein ☐ Ja

10. Verschiedene Personen sind zuständig für…

die Auftragserstellung	☐ Nein ☐ Ja
die Registrierung eingehender Waren	☐ Nein ☐ Ja
die Genehmigung für die Bezahlung von Waren	☐ Nein ☐ Ja
die Prüfung der Vertragspartner	☐ Nein ☐ Ja

11. Werden die Mitarbeiter im Geld- und Finanzbereich vor der Einstellung anhand von Zeugnissen oder Referenzen geprüft? ☐ Nein ☐ Ja

12. Gibt es besondere Vorgaben, um Betrug zu vermeiden? ☐ Nein ☐ Ja

Sind Lieferungen oder Leistungen an Neukunden ohne Vorkasse oder Vorleistung möglich? ☐ Nein ☐ Ja

Wenn ja, geben Sie bitte an, ob dies nur für Neukunden in Deutschland oder auch für Neukunden außerhalb Deutschlands gilt? ☐ Nein ☐ Ja

Werden Zahlungsanweisungen, Anfragen zu Bankdaten und -konten sowie Anweisungen zur Änderung von Kunden- oder Bankdaten immer im Vier-Augen-Prinzip geprüft und die Identität des Anfragenden überprüft? ☐ Nein ☐ Ja

Wenn ja, nehmen Sie eine Rückbestätigung der Anweisung oder Anfrage immer auf einem anderen Kommunikationsweg als dem der Anweisung oder Anfrage und mit den bereits hinterlegten (Kunden-)Daten vor (z. B. Anfrage per E-Mail und Rückbestätigung per hinterlegter Telefonnummer)? ☐ Nein ☐ Ja

Haben Sie für die Betrugsvermeidung interne Anweisungen oder Richtlinien erstellt und sind die zuständigen Mitarbeiter dazu geschult und sensibilisiert worden? ☐ Nein ☐ Ja

H. Datenschutz

Datenschutzhinweise (gilt nur, soweit die EU-DSGVO Anwendung findet)

1. Ich kann der Verarbeitung oder Nutzung meiner personenbezogenen Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung jederzeit mit Wirkung für die Zukunft widersprechen.
2. Schließlich erkläre ich, dass mir die Möglichkeit gegeben wurde, von dem Merkblatt zur Datenverarbeitung Kenntnis zu nehmen. Das Merkblatt ist unter http://www.ruv.de/datenschutz abrufbar.

Information zu Bonitätsauskünften und Scoring

Die R+V Allgemeine Versicherung AG ist Mitglied des Vereins Creditreform Wiesbaden, Adolfsallee 34, 65185 Wiesbaden. Bei dieser Versicherung nutzen wir Bonitätsinformationen und den Score-Wert, die wir von den im Verband der Vereine Creditreform zusammengeschlossenen Auskunfteien erhalten. In den uns übermittelten Score-Wert fließen die dort über Sie gespeicherten Daten, einschließlich der Adressdaten, ein und werden bewertet. Beim Scoring ist keine Information alleinige Grundlage. Die Bewertung ergibt sich immer aus der Kombination aller zugrundegelegten Faktoren. Der Score-Wert gibt die Wahrscheinlichkeit an, mit der Sie Ihren finanziellen Verpflichtungen nachkommen können. Sie erfahren bei dem für den Sitz Ihres Unternehmens zuständigen örtlichen Verein Creditreform, ob ein Eintrag über Sie vorliegt.

Informationspflicht, wenn wir Daten Dritter von Ihnen erhalten

Ich verpflichte mich, Dritte nach der EU-DSGVO zu informieren, deren personenbezogene Daten ich der R+V mitteile oder mitteilen lasse.

I. Auskünfte, Bestätigung und Unterschrift

Bevor Sie diesen Risikofragebogen unterschreiben, lesen Sie bitte die nachfolgende Seite sorgfältig durch. Diese enthält den Hinweis auf die Rechtsfolgen der Verletzung einer vorvertraglichen Anzeigepflicht und die Allgemeinen Hinweise.

Ich bestätige, dass die Angaben in diesem Risikofragebogen vollständig und richtig sind.

Ich bitte die R+V auf Grundlage meiner Angaben sowie der beigefügten Anlagen, mir ein Angebot für eine R+V-WirtschaftsschutzPolice zu unterbreiten.

Ich erkläre mich damit einverstanden, dass meine Angaben im Fall eines Vertragsabschlusses Grundlage und Bestandteil des Versicherungsvertrags werden.

Ort, Datum	Unterschrift und Firmenstempel
Ort, Datum	Unterschrift Vermittler

Mitteilung nach § 19 Absatz 5 Versicherungsvertragsgesetz (VVG) über die Folgen einer Verletzung der gesetzlichen Anzeigepflicht

Damit wir Ihren Risikofragebogen ordnungsgemäß prüfen können, ist es notwendig, dass Sie die gestellten Fragen wahrheitsgemäß und vollständig beantworten. Es sind auch solche Umstände anzugeben, denen Sie nur geringe Bedeutung beimessen. Bitte beachten Sie, dass Sie Ihren Versicherungsschutz gefährden, wenn Sie unrichtige oder unvollständige Angaben machen. Nähere Einzelheiten zu den Folgen einer Verletzung der Anzeigepflicht können Sie der nachstehenden Information entnehmen.

Welche vorvertraglichen Anzeigepflichten bestehen?
Sie sind bis zur Abgabe Ihrer Vertragserklärung verpflichtet, alle Ihnen bekannten gefahrerheblichen Umstände, nach denen wir in Textform gefragt haben, wahrheitsgemäß und vollständig anzuzeigen. Wenn wir nach Ihrer Vertragserklärung, aber vor Vertragsannahme in Textform nach gefahrerheblichen Umständen fragen, sind Sie auch insoweit zur Anzeige verpflichtet.

Welche Folgen können eintreten, wenn eine vorvertragliche Anzeigepflicht verletzt wird?

1. Rücktritt und Wegfall des Versicherungsschutzes
Verletzen Sie die vorvertragliche Anzeigepflicht, können wir vom Vertrag zurücktreten. Dies gilt nicht, wenn Sie nachweisen, dass weder Vorsatz noch grobe Fahrlässigkeit vorliegt. Bei grob fahrlässiger Verletzung der Anzeigepflicht haben wir kein Rücktrittsrecht, wenn wir den Vertrag auch bei Kenntnis der nicht angezeigten Umstände, wenn auch zu anderen Bedingungen, geschlossen hätten. Im Fall des Rücktritts besteht kein Versicherungsschutz.

Erklären wir den Rücktritt nach Eintritt des Versicherungsfalls, bleiben wir dennoch zur Leistung verpflichtet, wenn Sie nachweisen, dass der nicht oder nicht richtig angegebene Umstand weder für den Eintritt oder die Feststellung des Versicherungsfalls noch für die Feststellung oder den Umfang unserer Leistungspflicht ursächlich war. Unsere Leistungspflicht entfällt jedoch, wenn Sie die Anzeigepflicht arglistig verletzt haben.

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

2. Kündigung
Können wir nicht vom Vertrag zurücktreten, weil Sie die vorvertragliche Anzeigepflicht lediglich einfach fahrlässig oder schuldlos verletzt haben, können wir den Vertrag unter Einhaltung einer Frist von einem Monat kündigen. Unser Kündigungsrecht ist ausgeschlossen, wenn wir den Vertrag auch bei Kenntnis der nicht angezeigten Umstände, wenn auch zu anderen Bedingungen, geschlossen hätten.

3. Vertragsänderung
Können wir nicht zurücktreten oder kündigen, weil wir den Vertrag auch bei Kenntnis der nicht angezeigten Gefahrumstände, wenn auch zu anderen Bedingungen, geschlossen hätten, werden die anderen Bedingungen auf unser Verlangen Vertragsbestandteil.

Haben Sie die Anzeigepflicht fahrlässig verletzt, werden die anderen Bedingungen rückwirkend Vertragsbestandteil. Haben Sie die Anzeigepflicht schuldlos verletzt, werden die anderen Bedingungen erst ab der laufenden Versicherungsperiode Vertragsbestandteil.

Erhöht sich durch die Vertragsänderung der Beitrag um mehr als 10 % oder schließen wir die Gefahrabsicherung für den nicht angezeigten Umstand aus, können Sie den Vertrag innerhalb eines Monats nach Zugang unserer Mitteilung über die Vertragsänderung fristlos kündigen. Auf dieses Recht werden wir Sie in unserer Mitteilung hinweisen.

4. Ausübung unserer Rechte
Wir können unsere Rechte zum Rücktritt, zur Kündigung oder zur Vertragsänderung nur innerhalb eines Monats schriftlich geltend machen. Die Frist beginnt mit dem Zeitpunkt, zu dem wir von der Verletzung der Anzeigepflicht, die das von uns geltend gemachte Recht begründet, Kenntnis erlangen. Bei der Ausübung unserer Rechte haben wir die Umstände anzugeben, auf die wir unsere Erklärung stützen. Zur Begründung können wir nachträglich weitere Umstände angeben, wenn für diese die Frist nach Satz 1 nicht verstrichen ist. Wir können uns auf die Rechte zum Rücktritt, zur Kündigung oder zur Vertragsänderung nicht berufen, wenn wir den nicht angezeigten Gefahrumstand oder die Unrichtigkeit der Anzeige kannten. Unsere Rechte zum Rücktritt, zur Kündigung und zur Vertragsänderung erlöschen mit Ablauf von fünf Jahren nach Vertragsschluss. Dies gilt nicht für Versicherungsfälle, die vor Ablauf dieser Frist eingetreten sind. Die Frist beträgt zehn Jahre, wenn Sie die Anzeigepflicht vorsätzlich oder arglistig verletzt haben.

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

Allgemeine Hinweise

Sie tragen die Verantwortung für die Richtigkeit und Vollständigkeit aller Angaben, auch dann, wenn Sie diese nicht eigenhändig geschrieben haben. Striche oder sonstige Zeichen anstelle der Worte sowie Nichtbeantwortung der Fragen gelten als Verneinung. Unrichtige Beantwortung der Fragen nach Gefahrumständen sowie arglistiges Verschweigen auch sonstiger Gefahrumstände kann uns berechtigen, den Versicherungsschutz zu versagen. Mündliche Nebenabreden sind unwirksam.

Die selbständige Abgabe von (vorläufigen) Deckungszusagen ist den Vermittlern verboten und ohne rechtliche Wirkung für uns.

R+V Allgemeine Versicherung AG, Vorsitzender des Aufsichtsrats: Generaldirektor Dr. Norbert Rollinger.
Vorstand: Dr. Klaus Endres, Vorsitzender; Jens Hasselbächer, Tillmann Lukosch, Julia Merkel, Marc René Michallet.
Sitz: Raiffeisenplatz 1, 65189 Wiesbaden, Handelsregister Nr. HRB 2188, Amtsgericht Wiesbaden, USt-IdNr. DE 811198334