

Versicherungsnehmer:

Beratung durch:

OPTICON Beratungs- und Finanzdienstleistungs GmbH

Hauptstr. 24 • 67273 Weisenheim am Berg

Tel.: 06353/5080200

Fax: 06353/5080201

info@opticon-bfg.de

http://www.opticon-bfg.de/

Persönlicher Ansprechpartner:

1. Angaben zum Unternehmen	
1.1. Firmierung und Anschrift	☐ wie oben angegeben ☐ abweichend
1.2. Homepage und E-Mailadresse	☐ nicht vorhanden
1.3. Betriebs-/Tätigkeitsbeschreibung	
1.4. Gibt es mitzuversichernde Unternehmen im In- und Ausland?	☐ nein ☐ ja Wenn ja, Namen und Anschriften der Unternehmen?

1.5. Jahresumsätze d. letzten Geschäftsjahres in € Umsatz gesamt davon USA/Kanada-Anteil	€ €
2. Gewünschter Versicherungsumfang	
2.1. gewünschte Versicherungssumme	☐ 125.000 € ☐ 250.000 € ☐ 500.000 € ☐ 750.000 € sonstige: €
3. Elektronischer Zahlungsabwicklung (Payment processing)	
3.1. Akzeptieren Sie EC- / Kreditkarten?	☐ nein ☐ ja wenn ja, welche und wie hoch ist der Umsatzanteil (in %)?
3.2. Welche Umsätze werden über Online-Handel (E-Commerce) getätigt?	☐ nein ☐ ja wenn ja, welche und wie hoch ist der Umsatzanteil (in %)?
3.3. Erfüllt Ihr Unternehmen die Vorgaben des Payment Card Industry Data Security Standard (PCI-Standard)?	☐ nein ☐ ja wenn ja, bitte Zertifikat beifügen!
3.4. Speichern Sie Kreditkartendaten auf Ihrem Netzwerk, wenn auch nur kurzfristig?	☐ nein ☐ ja wenn ja, ☐ verschlüsselt ☐ unverschlüsselt
4. Angaben zur Art und Menge der Daten	Bitte vervollständigen Sie die nachfolgenden Angaben hinsichtlich der Art und Menge von Daten, die Sie übertragen, bearbeiten, speichern etc., und in Bezug auf die vorhandene Datensicherheit:
4.1. Art der Daten, die übertragen, bearbeitet oder gespeichert werden sowie die maximale Anzahl der Daten die auf Ihrem Netzwerk gespeichert werden?	☐ Sozialversicherungs-, Führerschein- oder Ausweisdokumente max. Anzahl ☐ Steuer- oder Finanzdaten max. Anzahl ☐ Kreditkarten- / EC-Kartendaten max. Anzahl ☐ andere personenbezogene Daten max. Anzahl ☐ weitere Daten max. Anzahl

4.2. Sind die Daten verschlüsselt, solange Sie auf Ihrem Netzwerk gespeichert werden und/oder während der Dauer der Versendung innerhalb und außerhalb des Netzwerkes (einschl. W-LAN, in file transfers und E-Mails)?	☐ nein ☐ ja wenn nein, welche nicht?
4.3. Sind die Daten auf Laptops, PDAs und anderen mobilen Computern sowie mobilen Datenträgern, wie z. B. USB-Sticks, DVDs etc. verschlüsselt?	☐ nein ☐ ja wenn nein, welche nicht?
Wenn Sie externe Anbieter zur Datenspeicherung / -sicherung / -verarbeitung nutzen:	
4.4. Werden IT-Prozesse ausgelagert und/oder an externe IT-Dienstleister gegeben?	☐ nein ☐ ja wenn ja, welche Prozesse und an wen?
4.5. Stellen Sie sicher, dass diese Anbieter die Daten zu jeder Zeit verschlüsseln?	☐ nein ☐ ja wenn ja, Details zu zusätzlichen Sicherungsmaßnahmen
5. Angaben zur Datensicherung	
5.1. In welchen Intervallen werden die Daten gesichert und erfolgt die Sicherung zentral (Server)?	☐ nein ☐ ja ☐ täglich ☐ wöchentlich ☐
6. Angaben zu Zugriffskontrollen	
6.1. Beschränken Sie den Zugriff auf Daten auf den Personenkreis, welcher Zugriff auf diese Daten benötigt?	☐ nein ☐ ja

6.2. Dürfen Mitarbeiter eigenständig Software installieren oder nicht firmeneigene Datenträger (z.B. USB-Stick) an Firmenhardware anschließen?	☐ nein ☐ ja
7. Angaben zum Datenschutz	
7.1. Gibt es einen Datenschutzbeauftragten (auch extern) und eine schriftliche Datenschutzrichtlinie?	☐ nein ☐ ja
7.2. Gibt es einen IT-Sicherheitsbeauftragten?	☐ nein ☐ ja wenn ja, weitere Angaben zu dessen Aufgaben:
7.3. Nutzen und unterhalten Sie eine Firewall, um die Daten zu schützen?	☐ nein ☐ ja
7.4. Führen Sie Berichte, um festzuhalten, welche Art von Daten Sie speichern und wo diese gespeichert werden?	☐ nein ☐ ja
7.5. Gibt es ein System, welches die Art und Menge der Daten, die in Ihr Netzwerk gelangen, überwacht?	☐ nein ☐ ja
7.6. Gibt es ein System, welches die Art und Menge der Daten, die Ihr Netzwerk verlassen, überwacht?	☐ nein ☐ ja
7.7. Nutzen Sie eine Anti-Virus- Software und wird diese regelmäßig upgedatet?	☐ nein ☐ ja
7.8. Überwachen Sie Ihre Systeme, um entstehende Sicherheitslücken zu identifizieren und passen Sie Ihre Systeme und Anwendungen entsprechend an?	☐ nein ☐ ja
8. Angaben zum Schadenverlauf	
8.1. Wurde in den letzten 5 Jahren jemals Schadenersatzansprüche aufgrund IT-Angriffs und/oder Vorwurfs der Datenschutzverletzungen gegen Sie erhoben bzw. gab es jemals einen Schaden (Datenverlust/-diebstahl und Betriebsunterbrechung etc.)?	☐ nein ☐ ja Wenn ja, bitte erläutern Sie diesen:
8.2. Sind Ihnen Umstände bekannt, die zu einem Schadenersatzanspruch gegen Sie oder einem Schaden (Datenverlust, Betriebsunterbrechung etc.) führen könnten?	☐ nein ☐ ja Wenn ja, bitte erläutern Sie diese:

9. Sonstige Hinweise und Bemerkungen	
10. Risikorelevante Fragen und Belehrung	Bei den Fragen handelt es sich um Fragen über gefahrerhebliche Umstände. Unvollständige und unrichtige Angaben zu den gefahrerheblichen Umständen berechtigen den Versicherer, im Falle der vorsätzlichen oder grob fahrlässigen Verletzung der Anzeigepflicht, vom Versicherungsvertrag zurückzutreten. Wird die Anzeigepflicht vorsätzlich oder grob fahrlässig verletzt, hat der Versicherer das Recht, den Vertrag innerhalb eines Monats ab Kenntnis von der Anzeigepflichtverletzung unter Einhaltung einer Frist von einem Monat zu kündigen. Sie gestatten, dass die erfassten Daten nebst etwaigen Anlagen mittels unverschlüsselter E-Mail - auch über Dienstleister - an Versicherungsunternehmen zur Prüfung und Angebotserstellung weitergeleitet werden.
11. Unterschriften	
Datum, Unterschrift des Versicherungsmaklers	Datum, Unterschrift des Kunden
Interne Notizen Mitarbeiter: Datum : Uhrzeit: von bis	☐ telefonische Erfassung ☐ schriftliche Kundenangaben ☐ persönliche Besprechung ☐ im Maklerbüro ☐ beim Kunden ☐
Rev.001 vom 08.10.2014	