Maßstäbe / neu definiert

ZN/VD	BD	AB	Vermittler-Nr.
		00	

Fragebogen zur Risikoerfassung ByteProtect

Angaben zum Unternehmen (Versicherungsnehmer)

Name und Rechtsform: _____

Internetadresse: www._____ Kontaktperson: _____/ ☎ _____

Anschrift: _____

Sind Sie bereits Kunde der AXA? ( ) nein ( ) ja, Art der Versicherung: _____

Versicherungsschein-Nr.: _____

Jahr der Unternehmensgründung: _____

Zu welcher Branche ist Ihr Unternehmen zu rechnen (z. B. nach NACE)?

_____

Betriebsbeschreibung:

Wichtig für den Antragsteller:

Bitte beantworten Sie die Fragen vollständig und richtig, sonst ist der Versicherungsschutz gefährdet. Die Verletzung der vorvertraglichen Anzeigepflicht kann den Versicherer je nach Verschulden berechtigen, vom Vertrag zurückzutreten, ihn zu kündigen oder anzupassen, was zur Leistungsfreiheit des Versicherers - auch für bereits eingetretene Versicherungsfälle - führen kann.

Der Versicherer behält sich eine zusätzliche Risikoaufnahme vor Ort durch einen technischen Sachverständigen vor.

Allgemeine Informationen zur Verwendung Ihrer Daten und Ihrer diesbezüglichen Rechte finden Sie in dem Abschnitt „Information zur Verwendung Ihrer Daten“.

_____ _____

Ort, Datum Firma, Name, Unterschrift(en)

Funktion im Unternehmen: _____

A Allgemeine Angaben

Bitte machen Sie Angaben zu Ihrem Umsatz:

	Gesamtumsatz konsolidiert [EUR]	Davon in den USA [EUR]
Letztes Geschäftsjahr		
Aktuelles Geschäftsjahr (Erwartungswert)		

Weitere rechtlich selbständige Firmen im In- und Ausland sowie rechtlich unselbständige Betriebsstätten im Ausland. Bitte ggf. Beziehung erläutern (z. B. Joint Venture, 100 %-Tochter)

Firma/ Ort/ Land	Umsatz [EUR]	Tätigkeiten (Entwicklung, Vertrieb, Lager etc.)

Anteil des Umsatzes, der online (z. B. über Web-Shops) erzielt wird: _____ %

Unterliegt der Umsatz saisonalen Schwankungen? ( ) Nein

( ) Ja, Begründung: _____

Höchster Monatsumsatz: _____ EUR

Wie viele Mitarbeiter arbeiten in Ihrem Unternehmen im Jahresdurchschnitt?

Gesamt _____, freie Mitarbeiter _____, Studenten _____

Wer sind Ihre **Hauptkunden**? _____

Haben Sie mit einem Ihrer Kunden einen Umsatzanteil von mehr als 75 %?
( ) nein ( ) ja, _____ % mit _____

Sind Sie **mit Ihren Auftraggebern/Abnehmern** durch Personalunion, Gesellschaftsverhältnisse oder Beteiligungen **verbunden**? ( ) nein ( ) ja, mit _____

Anteil privater Kunden _____ %

Werden von Ihnen **personenbezogene Daten** gespeichert?

( ) Nein ( ) ja, und zwar folgende _____

Anzahl aktuell gespeicherter Datensätze: _____

Wo sehen Sie selber Ihr höchstes Risiko? Bitte erläutern:

B Bestehender Versicherungsschutz und Schadenverlauf

Aktuell bestehende Versicherungen

Bezeichnung	Anbieter	Versicherungssumme [EUR]
HaftpflichtV		
VertrauensschadenV		
ElektronikV		

Zum Schadenverlauf

Beschreibung der einzelnen Schäden, sofern diese einen Zusammenhang mit der EDV, dem Internet bzw. schutzbedürftigen Daten haben.

Beschreibung des Schadens (Ursache, Ablauf etc.)	Jahr	Aufwand [EUR]
Haftpflichtschäden		
Eigenschäden		

Welche IT-relevanten Sicherheitsvorfälle haben sich in Ihrem eigenen Unternehmen in den letzten drei Jahren ereignet, auch wenn diese zu keinem versicherten Schaden geführt haben (z. B. IT-Ausfälle, Schadsoftware-Befall, DDoS-Attacke, Hacking der Webseite, Verlust von sensiblen Daten, Beanstandungen von Datenschutzbehörden)?

Beschreibung des Vorfalls (Ursache, Ablauf etc.)	Jahr	Aufwand [EUR]

Sind Ihnen Umstände bekannt, die zu einem Schadenersatz gegen Sie oder zu einem Schaden führen könnten?

( ) Nein ( ) Ja, und zwar folgende: _____

C Gewünschter Versicherungsschutz

Versicherbare Bausteine		Versicherungs-summe [EUR]	Versicherungs-wunsch	
			Ja	Nein
A Ertragsausfall aufgrund folgender Gefahren:				
a)	Ausfall des Telekommunikationsnetzes oder der Webseite		☐	☐
b)	Bedienungsfehler durch eigene Mitarbeiter		☐	☐
c)	Denial of Service - Angriff		☐	☐
d)	Hacker-Angriff		☐	☐
e)	Manipulation durch eigene Mitarbeiter		☐	☐
f)	Ausfall einer IT-Dienstleistung (z. B. Cloud Computing)		☐	☐
B Sachverständigenkosten			☐	☐
C Datenwiederherstellung			☐	☐
D Rufschädigung / Krisenmanagement			☐	☐
E Datenschutzverletzung			☐	☐
F Internet-Betrug			☐	☐
G Erpressung			☐	☐
H Cyber-Haftpflicht			☐	☐
Jahreshöchstentschädigung				

Ist die Versicherung folgender Optionen gewünscht?

( ) **PCI-DSS-Vertragsstrafen (Sublimitiert!)**

„Es besteht Versicherungsschutz für PCI-Vertragsstrafen, die der Versicherungsnehmer wegen einer Verletzung der Payment Card Industry Data Security-Standards (PCI-DSS) aufgrund eines versicherten Schadens im Zusammenhang mit Kreditkartendaten zu leisten verpflichtet ist."

Ihr Versicherungssummenwunsch: _____ EUR

Zu Baustein H

( ) **Exporte in die und Leistungen in den USA/US-Territorien**

Art der Exporte und Leistungen: _____

Zu Baustein A f)

Folgende **externe IT-Dienstleister** sollen in die Ertragsausfallversicherung im Baustein A mit aufgenommen werden.

_____ mit folgenden Diensten: _____

_____ mit folgenden Diensten: _____

D Eigene IT-Infrastruktur

Ihr Unternehmen verfügt über:

( ) **eigene IT-Abteilung** mit _____ Mitarbeiter(n)

( ) **externe IT-Dienstleister** für folgende Leistungen:

- ( ) Datenspeicherung und –sicherung
- ( ) Web-Hosting
- ( ) Cloud Computing (für folgende Dienste: _____)
- ( ) Administration, technischen Support, Hotline
- ( ) _____
- ( ) Mit diesen wurden schriftliche Dienstleistungsverträge abgeschlossen.
  Bitte legen Sie Auszüge zu haftungsrechtlichen Regelungen bei.
- ( ) Es wurden keine Regressverzichtserklärungen bzw. Freistellungen ausgesprochen
  (wenn doch, bitte Dokumente vorlegen)
- ( ) Von den beauftragten IT-Dienstleistern wurden Bestätigungen über vorhandene
  IT-Haftpflichtversicherung eingeholt

( ) **eigenes Rechenzentrum** / Serverraum (Ort: _____)

( ) PC-Arbeitsplätze, Anzahl: _____

( ) internes, eigenes **Firmennetzwerk**
Anbindung von externen Standorten erfolgt durch: _____

( ) **Einwahlmöglichkeit** für Mitarbeiter in das interne Netzwerk über VPN
(Anzahl der Mitarbeiter mit einer derartigen Berechtigung: ____)

( ) eigene **Webseite**, die

- ( ) vom eigenen Server gehostet wird
- ( ) von _____ gehostet wird
- ( ) für das Web-Design und Aktualisierungen ist verantwortlich: _____

( ) Erlaubnis der Mitarbeiter, dass eigene Geräte eingebunden werden können (**BYOD**[1])

( ) Möglichkeiten, dass Kunden über das Internet bei Ihnen Käufe/Bestellungen tätigen können (**e-Commerce**)

- ( ) Hierbei werden **Kreditkartenzahlungen** zugelassen;
  Anzahl der gespeicherten Kreditkarten-Datensätze: _____

  Wenn ja, welcher Sicherheitsstandard ist hierbei gewährleistet? _____
  ( ) Dieser Standard ist zertifiziert seit _____

[1] BYOD = Bring Your Own Device – Private Geräte können verwendet und mit der EDV des Unternehmens verbunden werden/Datenaustausch betreiben

E Schutzmaßnahmen zur IT- bzw. Informationssicherheit

Sie haben in Ihrem Unternehmen folgende Maßnahmen zur IT- bzw. Informationssicherheit ergriffen:

( ) Schriftliche **Security Policy** (Festlegung von Sicherheitszielen und einer Sicherheitspolitik)

( ) Informationssicherheits-Managementsystem (**ISMS**) ist seit _____ im Unternehmen eingeführt
- ( ) Zertifizierung nach ISO/IEC 27001, BSI-Grundschutz oder vergleichbaren IT-Standards
- ( ) ITIL
- ( ) _____

( ) Zertifiziertes **Qualitätsmanagementsystem** (QMS) nach ISO 9001

Bitte weisen Sie Zertifizierungen durch entsprechende Kopien nach.

( ) Bestellung eines **Beauftragten** für IT-/Informationssicherheit

( ) Bestellung eines **Datenschutzbeauftragten** gemäß gesetzlicher Vorgaben
( ) intern ( ) extern

( ) Einrichtung eines **Patch-Managements**

( ) **Verschlüsselung** bzw. Zugriffssicherheit durch Passworteingabe für sensible Daten

( ) Dokumentierte und abgestufte **Berechtigungen** für Zugriff auf sensible Daten

( ) Regelmäßige **Datensicherung**
- ( ) Es erfolgen mindestens täglich Datensicherungen
- ( ) Die Datensicherungen werden getrennt und geschützt z. B. vor Brand gelagert
- ( ) Es werden regelmäßig Restore-Tests der Datenbestände durchgeführt

( ) Etablierung eines **Informationssicherheitsprozesses** (ISP)

( ) **Schutzbedarfsanalyse** ist erfolgt (zuletzt: _____)

( ) Schulungsplan zur Sicherstellung eines ausreichenden Bewusstseins der Mitarbeiter für das Thema Informationssicherheit (**Awareness-Schulungen**)

( ) Einsatz aktueller **Antiviren-Software und Firewalls**

( ) Installation eines **Intrusion Prevention-Systems**

( ) **Zugangssicherung** zu Rechenzentren und Serverräumen durch _____

( ) Speicherung von **Log-Files**, über die ein Zugriff auf Daten nachvollzogen werden kann.
Aufbewahrungszeit der Log-Files: ____ Tage/Monate

( ) Durchführung von **IT-Sicherheitsaudits** durch _____, zuletzt am _____

( ) **Penetrationstest** durch einen externen Sachverständigen, zuletzt am _____

( ) Sie verfügen über einen aktuellen **Notfallplan**, der Maßnahmen zur Bewältigung von Krisensituationen bzw. IT-Sicherheitsvorfällen (z. B. Cyber-Angriff, Ausfall des Internets etc.) festlegt.

Der Notfallplan wurde eingeführt am: _____

Der Notfall wurde zuletzt geprobt am: _____

Bitte Kopie des Notfallplanes vorlegen.

( ) Sie verfügen über externe Unterstützung im Krisen-/Notfall

über folgende Dienstleister: _____

F Bausteinspezifische Fragen

Eine Beantwortung der Fragen ist nur erforderlich, falls der jeweilige Baustein versichert werden soll.

Zu Baustein A – Ertragsausfall

Nach Ihrer Einschätzung dauert der **Wiederanlauf** aller Geschäftsprozesse nach einem vollständigen Netz- bzw. Serverausfall maximal _____ Stunden

Durchführung einer **Business Impact Analyse** (BIA) ( ) bislang nicht erfolgt

( ) zuletzt durchgeführt am _____

Maximal tolerierbare Ausfallzeit: _____

Prozess mit der geringsten tolerierbaren Ausfallzeit: _____

Ein **Business Continuity Management** (BCM) wurde eingeführt am _____

( ) nach ISO 22301

( ) nach folgendem Standard: _____

Ist ein „**Notbetrieb**“ vorgesehen bzw. möglich?

( ) Nein

( ) Ja, in folgendem Umfang: _____

Zu Baustein F – Internet-Betrug

Ist bei Ihnen sichergestellt, dass der Online-Banking-Standard HBCI mit elektronischer Signatur eingehalten wird?

( ) Ja

( ) Nein, Erläuterung: _____

Weitere Anmerkungen:

Sofern vorhanden, möchten wir Sie bitten, folgende Unterlagen dem ausgefüllten Fragebogen in Kopie beizufügen.

Unterlage	Liegt bei	Entfällt
Organigramm / Organisationsdarstellung	☐	☐
Firmen- und Produktbroschüren, ggf. Kataloge	☐	☐
Aktueller Geschäftsbericht	☐	☐
Haftungsrechtlich relevante Regelungen mit IT-Dienstleistern	☐	☐
Zertifikate	☐	☐
Security Policy	☐	☐
Notfallplan	☐	☐
	☐	☐

Fragebogen speichern | Fragebogen drucken | Eingaben löschen

Versand per E-Mail: it-check@axa.de

Information zur Verwendung Ihrer Daten

Maßstäbe / neu definiert

Zur Einschätzung des zu versichernden Risikos vor dem Abschluss des Versicherungsvertrags, zur Durchführung des Vertragsverhältnisses, insbesondere im Leistungsfall, benötigen wir personenbezogene Daten von Ihnen. Die in dem Antrag genannte Gesellschaft ist dabei die für die Datenverarbeitung verantwortliche Stelle für Ihre Daten.

Die Verarbeitung und Nutzung dieser Daten ist gesetzlich geregelt. Die deutsche Versicherungswirtschaft hat sich in den Verhaltensregeln der deutschen Versicherungswirtschaft verpflichtet, nicht nur die gesetzlichen Vorgaben einzuhalten, sondern auch darüber hinaus weitere Maßnahmen zur Förderung des Datenschutzes zu ergreifen. Erläuterungen dazu können Sie den Verhaltensregeln entnehmen, die Sie im Internet unter www.axa.de abrufen können. Ebenfalls im Internet abrufen können Sie Listen der Unternehmen unserer Gruppe, die an einer zentralisierten Datenverarbeitung teilnehmen sowie Listen der Auftragnehmer und der Dienstleister. Auf Wunsch händigen wir Ihnen auch gern einen Ausdruck dieser Listen aus. Soweit die Verarbeitung Ihrer Daten auf der Grundlage einer ausdrücklichen Einwilligungs- oder Schweigepflichtentbindungserklärung erfolgt, können Sie diese jederzeit widerrufen. Des Weiteren können Sie Auskunft über die zu Ihrer Person gespeicherten Daten beantragen sowie die Berichtigung Ihrer Daten verlangen, wenn diese unrichtig oder unvollständig sind. Ansprüche auf Löschung oder Sperrung Ihrer Daten können bestehen, wenn deren Erhebung, Verarbeitung oder Nutzung sich als unzulässig oder nicht mehr erforderlich erweist. Diese Informationen gelten auch für die versicherte Person. Wenn die versicherte Person nicht zugleich Versicherungsnehmer ist, wird der Versicherungsnehmer diese Informationen der versicherten Person weiter geben.
In allen diesen Fällen können Sie sich jederzeit an den AXA Konzern, Colonia-Allee 10-20, 51067 Köln, telefonisch an 0221/148 52900, oder per Email an datenschutz@axa.de wenden.

Hinweis auf die Möglichkeit des Widerspruchs gegen die Datenverwendung zur Werbung sowie Markt- und Meinungsforschung
Ihre personenbezogenen Daten werden ohne Ihre ausdrückliche Einwilligung zur Werbung für unsere eigenen Versicherungsprodukte und für andere Produkte der Unternehmen der AXA-Gruppe und deren Kooperationspartner sowie zur Markt- und Meinungsforschung unseres Unternehmens verwendet. Dem können Sie jederzeit formlos widersprechen.

Hinweis auf möglichen Datenaustausch mit dem Hinweis- und Informationssystem (HIS)
Die informa Insurance Risk and Fraud Prevention GmbH betreibt das Hinweis- und Informationssystem der Versicherungswirtschaft (HIS). An das HIS melden wir - ebenso wie andere Versicherungsunternehmen - erhöhte Risiken sowie Auffälligkeiten, die auf Versicherungsbetrug hindeuten könnten und daher einer näheren Prüfung bedürfen. Die Meldung ist bei Antragstellung oder im Schadenfall möglich und kann eine Person oder eine Sache, z. B. ein Kfz, betreffen. Eine Meldung zur Person ist möglich, wenn ungewöhnlich oft Schäden gemeldet werden oder z. B. das Schadenbild mit der Schadenschilderung nicht in Einklang zu bringen ist. Die Versicherer müssen im Schadenfall wissen, ob ein Fahrzeug schwerwiegende oder unreparierte Vorschäden hatte oder sogar schon einmal als gestohlen gemeldet wurde. Aus diesem Grund melden wir Fahrzeuge an das HIS, wenn diese einen Totalschaden haben, gestohlen worden sind, sowie im Falle von Abrechnungen ohne Reparaturnachweis. Immobilien melden wir an das HIS, wenn wir eine ungewöhnlich hohe Schadenhäufigkeit feststellen. Sollten wir Sie, Ihre Immobilie oder Ihr Fahrzeug an das HIS melden, werden Sie in jedem Fall über die Einmeldung von uns benachrichtigt.
Bei der Prüfung Ihres Antrags auf Abschluss eines Versicherungsvertrages oder Regulierung eines Schadens, richten wir Anfragen zur Person oder Sache (z. B. Kfz) an das HIS und speichern die Ergebnisse der Anfragen. Im Schadensfall kann es nach einem Hinweis durch das HIS erforderlich sein, genauere Angaben zum Sachverhalt von den Versicherern, die Daten an das HIS gemeldet haben, zu erfragen. Auch diese Ergebnisse speichern wir, soweit sie für die Prüfung des Versicherungsfalls relevant sind. Es kann auch dazu kommen, dass wir Anfragen anderer Versicherer in einem späteren Leistungsfall beantworten und daher Auskunft über Ihren Schadenfall geben müssen.
Eine detaillierte Beschreibung des HIS finden Sie im Internet unter www.informa-irfp.de.

Hinweis auf möglichen Datenaustausch mit anderen Versicherern
Wir möchten Sie darauf hinweisen, dass Sie als Antragsteller verpflichtet sind, uns Fragen zu Vorschäden oder Vorversicherungen vollständig und wahrheitsgemäß zu beantworten, da wir die Angaben im Rahmen der Risikoprüfung benötigen. Zur Überprüfung und Ergänzung Ihrer Angaben kann ein Datenaustausch mit anderen Versicherern erforderlich werden.

Hinweis für unternehmensbezogene Daten
Der Versicherer und dessen Dienstleistungsgesellschaften sind im erforderlichen Umfang berechtigt, unternehmensbezogene Daten, die sich aus den Antragsunterlagen oder der Vertragsdurchführung (Beiträge, Versicherungsfälle, Risiko-/Vertragsänderungen) ergeben, an Rückversicherer zur Beurteilung des Risikos und zur Abwicklung der Rückversicherung, sowie zur Beurteilung des Risikos und der Ansprüche an andere Versicherer und/ oder an den Gesamtverband der Deutschen Versicherungswirtschaft (GDV) zu übermitteln. Diese Berechtigung gilt unabhängig vom Zustandekommen des Vertrages sowie für entsprechende Prüfungen bei anderweitig beantragten Versicherungsverträgen und bei künftigen Anträgen. Die Unternehmen der AXA Konzern AG sind berechtigt, die allgemeinen Antrags-, Vertrags- und Leistungsdaten in gemeinsamen Datensammlungen zu führen und an die für den Versicherungsnehmer zuständigen Vermittler weiterzugeben, soweit dies der ordnungsgemäßen Durchführung seiner Versicherungsangelegenheiten dient.