Anhang Datensicherheit - BluJay

1. ALLGEMEINES

Dieser Anhang zur Datensicherheit des Unternehmens („**Anhang**“) beschreibt die logischen und physischen Sicherheitsanforderungen, die im Allgemeinen für die Erbringung von Dienstleistungen oder die Bereitstellung von Dienstleistungen oder Produkten für den Kunden im Rahmen des Vertrags („**Sicherheitsanforderungen**“) gelten. Sofern im Vertrag nichts anderes angegeben ist, gelten die Bedingungen dieses Anhangs und haben Vorrang vor allen widersprüchlichen oder unvereinbaren Bestimmungen, die im Vertrag festgelegt sind. Dies gilt allerdings unter der Voraussetzung, dass die im Vertrag festgelegten Sicherheitskontrollen gelten und Vorrang vor den Bestimmungen dieses Anhangs haben, wenn (i) der Vertrag dies ausdrücklich festlegt oder (ii) die im Vertrag festgelegten Sicherheitskontrollen die in diesem Anhang festgelegten übertreffen.

2. DEFINITIONEN

(i) „**Unternehmenspersonal**“ bezeichnet Mitarbeiter und Auftragnehmer des Unternehmens.

(ii) „**Vertrauliche Kundendaten**“ bezeichnet die Daten, die gemäß dem Vertrag als „vertrauliche Informationen“ gelten, sowie sämtliche personenbezogenen Daten, insbesondere sensible personenbezogene Daten.

(iii) „**Kundendaten**“ bezeichnet sämtliche Daten, die vom Kunden oder seinen autorisierten Benutzern an das Unternehmen übertragen oder von dem Unternehmen im Zusammenhang mit der Erbringung von Dienstleistungen im Rahmen des Vertrags abgerufen oder erworben werden.

(iv) „**Kundensysteme**“ bezeichnet die Systeme des Kunden, die vom Kunden verwaltet werden und auf die das Unternehmen im Zusammenhang mit der Bereitstellung von Software und/oder Dienstleistungen zugreift, einschließlich Computersysteme, Software und Netzwerke sowie der auf diesen Systemen, Software und Netzwerken gespeicherten oder über deren Nutzung zugänglichen Technologie und Daten.

(v) „**Datenmissbrauch**“ bezeichnet die unangemessene oder unrechtmäßige Ausübung des Rechts oder Privilegs, wie das Recht oder Privileg, auf Informationen zuzugreifen, die unrechtmäßige Offenlegung dieser Informationen oder die böswillige oder anderweitig unrechtmäßige Ausführung einer Funktion oder eines Vorgangs.

(vi) „**Branchenstandard(s)**“ bezeichnet Folgendes:

(A) Von einer großen Anzahl von Unternehmen angewandt oder übernommen, die in Größe, Gestalt und Funktion mit der Größe, Gestalt und Funktion des Unternehmens vergleichbar sind;

(B) Zur Anwendung durch ein maßgebliche im Inland anerkanntes Normungsinstitiut vorgeschrieben oder

(C) Von einer bedeutenden Anzahl anerkannter Experten auf diesem Gebiet als annehmbar und angemessen bewertet, es sei denn, eine kürzlich erfolgte Offenlegung/öffentliche Feststellung deckt einen erheblichen Fehler/eine Sicherheitslücke in einem solchen Standard auf.

(vii) „**Verlust**“ bedeutet den Verlust der Kontrolle über vertrauliche Informationen, sodass ein oder mehrere Akteure weiterhin solche Daten offenlegen bzw. den Datenmissbrauch ausführen können.

(viii) „**Privilegierte Benutzer**“ bezeichnet sämtliche Benutzer, die über erweiterte Berechtigungen für den Zugriff auf und die Konfiguration von Netzwerksystemen verfügen, einschließlich insbesondere Systemadministratoren und „Super-Benutzer“, die Anmeldeinformationen, Betriebssysteme, Quellcode, Anwendungen und andere Netzwerksysteme bereitstellen, installieren, aktualisieren oder ändern können.

(ix) „**Sensible personenbezogene Daten“** sind Informationen, die eine identifizierbare natürliche Person identifizieren oder sich auf diese beziehen (d. h. eine Person, die mittelbar oder unmittelbar identifiziert werden kann, einschließlich durch Verweis auf eine Identifikationsnummer, Standortdaten, eine Online-Kennung oder ein oder mehrere Faktoren, die für die physische, physiologische, psychische, wirtschaftliche, kulturelle oder soziale Identität der Person spezifisch sind) und ähnliche Daten, die nach anwendbarem Recht geregelt sind.

3. RICHTLINIEN, SENSIBILISIERUNG UND SCHULUNG

(a) Das Unternehmen unterhält und setzt dokumentierte Sicherheitsrichtlinien und -standards durch und veröffentlicht sie intern, die sich auf die Kernkonzepte der Datensicherheit beziehen, einschließlich Bestimmungen, die eine Bewertung verschiedener Risiken, Schwachstellen, Bedrohungen sowie die Verwaltung dieser Risiken vorschreiben, damit diese Maßgaben erfüllt und sämtliche anwendbaren Datenschutzgesetze und -vorschriften eingehalten werden.

(b) Das Unternehmen unterhält ein umfassendes schriftliches Datensicherheitsprogramm und aktualisiert und/oder überprüft dieses Programm nach Bedarf mindestens einmal im Jahr. Das Unternehmen trägt dazu bei, sicherzustellen, dass dieses Programm (x) den geltenden Gesetzen entspricht und sich an die geltenden Branchenstandards anpasst, (y) angemessene administrative, logische, technische und physische Sicherheitsvorkehrungen umfasst, die mit diesem Anhang übereinstimmen und (z) angemessen darauf ausgelegt ist, die folgenden Ziele zu erreichen:

(A) Die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von Kundendaten;

(B) Der Schutz vor Bedrohungen oder Gefahren für die Sicherheit und Integrität oder Verfügbarkeit von Kundensystemen und

(C) Unbefugten oder zufälligen Zugriff, Erwerb, Zerstörung, Verlust, Löschung, Offenlegung oder Änderung bzw. Nutzung von Kundendaten oder Kundensystemen zu verhindern.

(c) Ein oder mehrere qualifizierte Mitarbeiter des Unternehmens wurden mit der Verantwortung für die Pflege des Datensicherheitsprogramms des Unternehmens betraut. Das Programm wird von der Geschäftsleitung des Unternehmens zugelassen und genehmigt, um vertrauliche Kundendaten vor Verlust oder Missbrauch im Zusammenhang mit der Leistung des Unternehmens gemäß der geltenden vertraglichen Vereinbarung mit dem Kunden zu schützen.

(d) Wenn anwendbares Recht die Einhaltung von Sicherheitsanforderungen verhindert oder wenn anwendbares Recht strengere Anforderungen als die in diesem Anhang dargelegten vorgibt, wird das Unternehmen die anwendbaren Gesetze befolgen.

(e) Auf Anfrage wird das Unternehmen dem Kunden alle gemeinsam genutzten Hosting-Einrichtungen von Drittanbietern offenlegen, die Kundendaten enthalten und das Unternehmen wird zumutbare

Maßnahmen ergreifen, um sicherzustellen, dass diese Dritten die anwendbaren Bedingungen dieses Anhangs grundlegend einhalten.

(f) Das Unternehmen bietet seinem aktuellen Unternehmenspersonal jährlich Schulungen zu einem allgemeinen Spektrum von Themen der Datensicherheit an, insbesondere in Bezug auf Phishing und Social Engineering, Grundlagen der Sicherheit und Datenschutz und schult neues Unternehmenspersonal bei deren Einstellung bzw. Beauftragung. Für Unternehmenspersonal, das als privilegierter Benutzer gilt, bietet das Unternehmen eine obligatorische jährliche rollenspezifische Schulung in den Sicherheitsrichtlinien und -standards des Unternehmens an.

4. ZUGRIFFSKONTROLLE

(a) Das Unternehmen gestattet nur Unternehmenspersonal und Dritten, die für die Erbringung von vertragsgegenständlichen Dienstleistungen benötigt werden, den Zugriff auf Kundendaten oder Kundensysteme. Autorisiertes Unternehmenspersonal und Dritte benutzen Kundendaten oder Kundensysteme nur, wenn dies zur Erfüllung ihrer Verpflichtungen aus dem Vertrag und diesem Anhang erforderlich ist.

(b) Das Unternehmen wendet das „Prinzip des geringsten Privilegs (Principle of Least Privilege/PLP)“ für den Zugriff auf nur solche Informationen an, die sich auf Kundenvorgänge beziehen, die für die Ausübung einer rechtmäßigen Geschäftsfunktion erforderlich sind. Das Unternehmen setzt eine sichere und zuverlässige Methode zur Durchsetzung von Berechtigungskontrollen ein, um den Zugriff gemäß PLP zu beschränken. Die Einhaltung des PLP erfordert ein Verfahren, das den Zugriff von Unternehmenspersonal und Dritten, die keinen Zugriff mehr benötigen, um im Rahmen eines Vertrags zu arbeiten (z. B. ein gekündigter oder an anderer Stelle zugewiesener Mitarbeiter/Auftragnehmer), umgehend beendet.

(c) Das Unternehmen verfügt über ein dokumentiertes Verfahren zur Steuerung von Benutzer-IDs und anderen Kennungen, um sicherzustellen, dass sie für die Benutzer eindeutig sind und nicht gemeinsam genutzt werden.

(d) Das Unternehmen wird die anwendbaren Gesetze, die geltenden Branchenstandards und die Alterungsverfahren befolgen, um die Möglichkeiten für die Kompromittierung der Passwortsicherheit sowie für die Authentifizierung und Autorisierung von Benutzern zu begrenzen. Das Unternehmen benutzt keine gemeinsamen oder generischen Legitimationsmerkmale für den Zugriff auf Kundendaten oder Kundensysteme. Die eingesetzten Passwortverfahren unterstützen Folgendes:

(A) Passwörter bestehen aus mindestens acht (8) Zeichen und

(B) enthalten mindestens einen Buchstaben, ein numerisches Zeichen sowie ein Sonderzeichen.

(C) Darüber hinaus laufen Passwörter spätestens alle neunzig (90) Tage ab

(D) und Benutzer-IDs werden nach nicht mehr als zehn (10) fehlgeschlagenen Anmeldeversuchen deaktiviert.

(e) Das Unternehmen überprüft die Identität des Benutzers vor dem Zurücksetzen von Passwörtern und bevor Konten, die mehr als die 90 Tage lang inaktiv bleiben, deaktiviert werden.

(f) Soweit dies im Einzelfall praktikabel ist muss der Benutzer, nachdem sich eine Sitzung für mehr als fünfzehn (15) Minuten im Ruhezustand befindet, das Kennwort erneut eingeben und die Sitzung reaktivieren.

(g) Das Unternehmen überprüft und widerruft in regelmäßigen Abständen die Zugriffsrechte von Benutzern.

(h) Das Unternehmen stellt die vom Unternehmen verwalteten Legitimationsmerkmale über dokumentierte technische und logische Kontrollverfahren bereit und widerruft sie.

(i) Die Authentifizierung bei den Netzwerkressourcen, Plattformen, Servern, Workstations, Anwendungen und Geräten des Unternehmens ist mit Standardpasswörtern nicht zulässig, und wenn verfügbar, werden rollenbasierte Zugriffskontrollen verwendet.

(j) Der Zugriff auf Kundendaten und Kundensysteme erfolgt gegebenenfalls über eine gesicherte Verbindung zwischen den Servicestandorten des Unternehmens (einschließlich des Zugriffs über einen der Cloud-Service-Provider des Unternehmens) und dem Kunden.

5. SICHERER DATENSCHUTZ

(a) Das Unternehmen speichert vertrauliche Kundendaten nur auf Geräten, die diese Sicherheitsanforderungen erfüllen.

(b) Das Unternehmen verwendet branchenweit standardisierte Maßnahmen, einschließlich Verschlüsselung, um das Abfangen von oder den Zugriff auf vertrauliche(n) Informationen zu verhindern, die die Netzwerke durchqueren. Für die Übertragung über das öffentliche Internet und andere extern zugängliche Netze ist eine Verschlüsselung der Übertragung erforderlich.

(c) Vertrauliche Informationen, die in Papierform oder unverschlüsselten elektronischen Medien enthalten sind, werden in einem kontrollierten Raum (z. B. in einem einzelnen Büro mit Tür) mit standardmäßiger Verriegelung außerhalb der Geschäftszeiten oder in verschlossenen Aufbewahrungsbehältern (z. B. verschlossene Schublade, Schrank) aufbewahrt.

(d) Die Benutzung vertraulicher Kundendaten in einer nicht-Produktions- (Test- oder Entwicklungs-) Umgebung ist nur nach Zustimmung durch den Kunden zulässig.

(e) Das Unternehmen unterhält sichere Datenvernichtungsverfahren, einschließlich insbesondere der Benutzung sicherer Löschen-Befehle, Entmagnetisierung und "Crypto-Shredding", wenn nötig. Die Verfahren des Unternehmens folgen den Branchenstandards.

(f) Beim physischen Transport digitaler Medien mit vertraulichen Kundendaten werden diese Informationen durch Speicherverschlüsselung geschützt. Wenn vom Kunden genehmigt, Transport mit einem qualifizierten Kurier, mit Tracking und in einem physisch sicheren Behälter. Der physische Transport von Papierdokumenten oder anderen physischen Medien, die vertrauliche Kundendaten enthalten, muss vor der beiläufigen Beobachtung der Informationen durch Fremde geschützt und mit zuverlässigen Mitteln, einschließlich Tracking, gesendet werden.

(g) Wenn vertrauliche Kundendaten in einem Unternehmensserver oder in einem Rechenzentrum gespeichert oder verarbeitet werden, erfüllen diese Einrichtungen die in diesen Sicherheitsanforderungen festgelegten Kontrollen.

(h) Das Unternehmen verfügt über einen Standard für Verschlüsselung und Schlüsselverwaltung, der akzeptable Verschlüsselungsstandards für die Benutzung in Systemen und Umgebungen definiert. Dieser Standard dient zur Behebung von Problemen und zur Klärung von Verschlüsselungsproblemen, indem er spezifische Anforderungen identifiziert, die Informationsressourcen erfüllen müssen:

(A) Das Unternehmen verschlüsselt vertrauliche Kundendaten im Ruhezustand, bei der Übertragung und bei der Benutzung über AES mit mindestens 128-Bit-Verschlüsselung und 1024-Bit-Schlüssellänge.

(B) Vor der Sicherung werden alle Kundendaten verschlüsselt oder gleichwertig gesichert.

(C) Das Unternehmen wird bei der Übertragung von Kundendaten über das Internet branchenweit verfügbare Verschlüsselungsmethoden benutzen.

6. ENDPOINT- UND NETZWERKSICHERHEIT

(a) Das Unternehmen installiert, konfiguriert und verwaltet Perimeter- und Netzwerksicherheitskontrollen, um unbefugten Zugriff auf Kundendaten und/oder Kundensysteme zu verhindern.

(b) Das Unternehmen verwaltet und konfiguriert Endpoint Security-Software auf Servern, Desktops, Laptops, mobilen und tragbaren digitalen Mediengeräten. Der Schutz von Endgeräten kann Verschlüsselungssoftware, Systeme zur Erkennung von Vorfällen, Systeme zur Verhinderung von Vorfällen und Anti-Malware-Software gemäß Branchenstandards umfassen. Das Unternehmen trägt dazu bei, dass solche Konfigurationen Warnungen an das Unternehmen und Protokolle generieren, auf die das Unternehmen zugreifen kann.

(c) Das Unternehmen implementiert an geeigneten Stellen im Unternehmensnetzwerk Kontrollen nach Branchenstandard (sowohl hinsichtlich der Häufigkeit als auch der Art), um den Ein- und Ausgang von Kommunikation und Daten in Umgebungen zu kontrollieren, die vertrauliche Kundendaten enthalten.

(d) Das Unternehmen wird die etablierten Sicherheitskontrollen des Unternehmens nicht umgehen oder versuchen, diese zu umgehen, auch nicht beim Zugriff auf externe Netzwerke auf die Systeme des Kunden.

(e) Das Unternehmen implementiert und pflegt Sicherheits- und Härtungsstandards für Netzwerkgeräte, insbesondere in Bezug auf Basiskonfigurationen, Patching, Passwörter und Zugriffskontrolle.

(f) Das Unternehmen befolgt dokumentierte Änderungsmanagementverfahren.

(g) Das Unternehmen ändert die Standardpasswörter für Server, bevor Geräte oder Systeme in Produktion gehen.

(h) Das Unternehmen führt elektronische Protokolle über den Zugriff und Ereignisse, um die Bestätigung des Zugriffs und den Schutz der Daten zu gewährleisten. Protokolle werden vor unbefugtem Zugriff, Änderung und versehentlicher oder vorsätzlicher Zerstörung geschützt. Protokollprüfungen werden regelmäßig durchgeführt.

(i) Das Unternehmen schützt Workstations angemessen vor Eindringversuchen, indem es automatische Bildschirmschoner, Sperren von Geräten, Datenschutz-Bildschirme und/oder ähnliche Kontrollen implementiert.

7. ANWENDUNGSMANAGEMENT

(a) Unabhängig von der Entwicklungsmethodik unterhält das Unternehmen einen Software Development Life Cycle (SDLC)-Prozess, der Sicherheitscodierungsverfahren (z. B. OWASP Top 10) enthält.

(b) Anwendungsentwicklung, Test- und Produktionsaktivitäten werden getrennt.

(c) Der Zugriff auf und die Speicherung des Anwendungsquellcodes ist auf die Unterstützung des Prinzips der geringsten Privilegien (Principle of Least Privilege/PLP) beschränkt und wird in einem dedizierten System (Quellcode-Repository) verwaltet. Der Quellcode der Anwendung wird über die Versionskontrolle verwaltet.

(d) Die Anwendungsdokumentation wird auf dem neuesten Stand gehalten, in zugänglicher Form aufbewahrt und vor Verlust oder Beschädigung geschützt.

(e) Die intern entwickelte Software wird vor der Bereitstellung getestet, einschließlich ggf. Regressionstests.

8. RISIKOMANAGEMENT

(a) Das Unternehmen unterhält ein Risikobewertungsprogramm, in dem Rollen und Verantwortlichkeiten für die Durchführung der Risikobeurteilung und die Reaktion auf Ergebnisse definiert werden. Das Unternehmen führt eine jährliche Risikobewertung durch, um das Design von Kontrollmechanismen zum Schutz von Geschäftsabläufen und Informationstechnologie zu überprüfen.

(b) Das Unternehmen unterhält einen Risikobeurteilungswartungsplan, der die Problemverfolgung bis zum Abschluss umfasst und den Wartungsfortschritt regelmäßig anhand der Zieldaten misst. Für die Risikoakzeptanz wird die Unternehmensleitung eine klare Bestätigung und eine Beschreibung des Risikos bereitstellen. Die Risikoakzeptanz beinhaltet eine geschäftliche Rechtfertigung.

9. BETRIEBSMANAGEMENT

(a) Die Systeme und Geräte des Unternehmens, die an der Leistung eines Vertrags beteiligt sind, werden gemäß den festgelegten Baselines und Standards sicher verwaltet und konfiguriert. Das Unternehmen hat eine Software zur Erkennung von Viren und Malware nach Branchenstandard implementiert und verfügt über ein Upgrade-Intervall.

(b) Das Unternehmen wendet Sicherheitspatches und Systemaktualisierungen auf vom Unternehmen verwalteter Software und Anwendungen, Geräten und Betriebssystemen in einem angemessenen Zeitrahmen an, basierend auf der Wichtigkeit der Sicherheitsanfälligkeit, der Verfügbarkeit des Patches und der Sensibilität der zugrunde liegenden Daten. Patches werden dem Kunden bei Verfügbarkeit zur Verfügung gestellt, wobei der folgende Zeitplan die zulässigen Grenzen für das Testen und Anwenden von Patches definiert.

(i) Das Unternehmen führt regelmäßige Sicherheitsschwachstellenanalysen von Systemen und Netzwerken des Unternehmens durch.

(ii) Jährlich führt das Unternehmen Tests zur Netzdurchdringung externer Netzwerke durch.

(iii) Das Unternehmen identifiziert, ermittelt, dokumentiert und beseitigt Schwachstellen und Bedrohungen für Kundendaten und Kundensysteme.

(iv) Das Unternehmen wendet Sicherheitspatches und Systemaktualisierungen auf vom Unternehmen verwalteter Software und Systemen, Geräten und Betriebssystemen in einem angemessenen Zeitrahmen an, basierend auf der Wichtigkeit einer identifizierten Schwachstelle, der Verfügbarkeit des Patches und der Sensibilität der zugrunde liegenden Daten.

10. GESCHÄFTSKONTINUITÄT UND NOTFALLWIEDERHERSTELLUNG

(a) Das Unternehmen unterhält ein dokumentiertes Geschäftskontinuitätsprogramm (Business Continuity Program/BCP). Das Unternehmen wird seine BCP-Pläne mindestens jährlich überprüfen.

11. VERWALTUNG VON UND REAKTION AUF SICHERHEITSVORFÄLLE(N)

(a) Im Rahmen des Datensicherheitsprogramms führt das Unternehmen einen dokumentierten Plan zur Verwaltung von und Reaktion auf Sicherheitsvorfälle(n) im Falle einer tatsächlichen oder vermuteten Sicherheitskompromittierung durch und aktualisiert diesen jährlich.

(b) Der Plan zur Verwaltung von und Reaktion auf Sicherheitsvorfälle(n) des Unternehmens enthält dokumentierte formale Verfahren, die den Branchenstandards und den geltenden Gesetzen zur Untersuchung von und Reaktion auf Sicherheitsvorfälle(n) entsprechen, einschließlich insbesondere behördliche Benachrichtigungen im Falle von Datenschutzverletzungen.

(c) Das Unternehmen kooperiert in zumutbarer Weise mit dem Kunden bei Untersuchungen über eine mögliche betrügerische oder unbefugte Nutzung oder den Zugriff auf Kundendaten oder Kundensysteme durch Mitarbeiter des Unternehmens bzw. durch Dritte.

(d) Wenn das Unternehmen eine Sicherheitsverletzung entdeckt oder darüber informiert wird, die zu unberechtigtem Zugriff, Erwerb, Offenlegung oder Nutzung von Kundendaten oder Kundensystemen oder einer Verletzung dieser Sicherheitsanforderungen führt, wird das Unternehmen den Kunden so schnell wie möglich benachrichtigen.

(e) Der Nachtrag zur Datenverarbeitung beschreibt weitere Maßnahmen, die das Unternehmen im Falle einer Sicherheitsverletzung ergreifen wird.

12. PHYSISCHE SICHERHEIT

Das Unternehmen setzt die folgenden physischen Sicherheitsmaßnahmen an Stellen ein, wo vertrauliche Kundendaten gespeichert werden oder zugänglich sind.

(a) Das Unternehmen gestattet nur autorisierten Personen Zugang, die aus berechtigten geschäftlichen Gründen auf Einrichtungen und Bereiche des Unternehmens, in denen vertrauliche Kundendaten gespeichert oder zugänglich sind, zugreifen müssen.

(b) Systeme, die Facility Access Control (Einrichtungszutrittskontrolle) bieten, sind vor Manipulation, Umgehung oder Zerstörung geschützt, werden jederzeit in betriebsbereitem Zustand gehalten und aktualisiert oder geändert, wenn sie kompromittiert oder unwirksam werden.

(c) Die Facility Controls erfüllen oder übertreffen die geltenden Branchenstandards, um physische Kompromisse zu verhindern und zu erkennen.

(d) Das Unternehmen überprüft in regelmäßigen Abständen die Compliance der Facility Controls, um die Einhaltung von Compliance- und Sicherheitsanforderungen zu gewährleisten.

13. RECHT AUF PRÜFUNG (AUDIT)

(a) Der Kunde darf auf Wunsch und auf eigene Kosten nicht mehr als einmal pro Kalenderjahr (jährlich) die Einhaltung dieses Anhangs durch das Unternehmen in zumutbarer Weise prüfen. Eine solche Prüfung findet während der normalen Geschäftszeiten und -tage statt, wobei das Unternehmen mindestens 30 Werktage zuvor schriftlich darüber in Kenntnis gesetzt werden muss. Die Prüfung

kann vor Ort am Standort des Unternehmens oder aus der Ferne durchgeführt werden. Spätestens 2 Wochen vor Beginn der Prüfung vereinbaren Unternehmen und Kunde gemeinsam den Umfang und den Zeitplan für die Prüfung.

(b) Das Unternehmen kooperiert in zumutbarer Weise mit der Prüfung durch den Kunden, indem es dem Kunden Unterlagen zur Verfügung stellt, die die Einhaltung dieses Anhangs belegen.

(c) Auf Anfrage wird das Unternehmen sämtliche Prüfungsergebnisse mit dem Kunden besprechen und ggf. gemeinsam mit dem Kunden Maßnahmen und Fristen zur Behebung vereinbaren.

(d) auf Anfrage stellt das Unternehmen dem Kunden anstelle einer Prüfung einen jährlichen Sicherheitsfragebogen zur Verfügung (maximal eine (1) Anfrage innerhalb eines Zeitraums von zwölf (12) Monaten), in dem spezifische Fragen zum Datensicherheitsprogramm des Unternehmens wie zutreffend beantwortet werden.

ENDE DES ANHANGS