viastore
a TOYOTA AUTOMATED LOGISTICS company

Öffentliche Richtlinie

Partner Information Security and Data Protection

Policy

BESCHREIBUNG: **Referenzdokument für vertragliche Vereinbarungen mit Drittparteien.**

viastore GRUPPE

VERSION: **1.6**

SCHUTZKLASSE: **normal**

Guaranteed Success.

Inhalt

Dokumentinformationen / Änderungsstand

Datum	Version	Änderung	Autor
2025-04-10	1.0	Ursprüngliche Version.	Thorsten Sauter
2025-06-24	1.1	Aktualisierte Version.	Thorsten Sauter
2025-06-25	1.2	Kleine Korrekturen in der Sprache	Thorsten Sauter
2025-07-22	1.3	Partner Key Users	Thorsten Sauter
2025-07-27	1.4	EU Data Act, EU AI ACT	Thorsten Sauter
2025-05-27	1.5	Eigentumsrechte an KI	Thorsten Sauter
2025-08-07	1.6	Datenverarbeitung	Thorsten Sauter

1. Zweck

Diese Richtlinie definiert verbindliche Anforderungen an die Informationssicherheit und den Datenschutz in vertraglichen Vereinbarungen mit Drittpartnern, Lieferanten, Verkäufern und Dienstleistern (im Folgenden: "Partner"). Dieses Dokument dient neben anderen Maßnahmen der Umsetzung entsprechender gesetzlicher Verpflichtungen bzw. soll deren Umsetzung sicherstellen, u.a. NIS2 und Cyber Resilience Act (CRA), und zielt darauf ab, das Risiko für die kritischen Systeme, Daten und den Betrieb von viastore zu minimieren.

2. Geltungsbereich

Diese Richtlinie gilt für alle Partner, die an der Herstellung, Entwicklung oder Lieferung von Produkten oder Software mit digitalen Komponenten für **viastore** oder einen **viastore**-Kunden beteiligt sind. Sie gilt auch für Partner, deren nicht-digitale Waren oder Dienstleistungen für den gesamten Liefer- und Leistungsrahmen entscheidend sind, um die Vertragserfüllung zu gewährleisten und die Integrität der **viastore**-Lieferkette, die betriebliche Stabilität und die Kundenverpflichtungen zu schützen.

Darüber hinaus gilt die Richtlinie für alle Partner, die **viastore**-Daten, -Systeme oder -Dienstleistungen verarbeiten, übertragen, speichern oder darauf zugreifen - unabhängig davon, ob sie in lokalen, hybriden oder Cloud-basierten Umgebungen arbeiten.

Diese Richtlinie ersetzt oder gewährt keine zusätzlichen Berechtigungen, die über die in anderen Unternehmensrichtlinien, Vorschriften oder Anweisungen der Geschäftsleitung - insbesondere in Bezug auf die GDPR - festgelegt sind.

3. Anforderungen an die Vertraulichkeitsvereinbarung für Partner

Alle Partner müssen eine Vertraulichkeitsvereinbarung (NDA) unterzeichnen, bevor sie Zugang zu Informationen oder Daten erhalten. Dadurch wird sichergestellt, dass sensible Materialien geschützt sind und alle externen Mitarbeiter vertraglich zur Geheimhaltung verpflichtet sind.

4. Anforderungen an die Informationssicherheit

Partner, die in den definierten Geltungsbereich fallen, müssen alle geltenden Gesetze zur Informationssicherheit und zum Datenschutz einhalten sowie die in diesem Abschnitt dargelegten Kontrollen und Anforderungen einhalten.

4.1 Festlegung von Haupt- und Ersatzbenutzern für die Kontoverwaltung

Wenn **viastore** oder einer seiner Kunden Benutzerkonten für den Netzwerkzugang bereitstellt, muss der Partner einen autorisierten Hauptnutzer und einen Ersatznutzer benennen, die dafür verantwortlich sind, **viastore** über alle personellen Änderungen zu informieren. Die benannten Benutzer fungieren als primäre und sekundäre Ansprechpartner für alle kontobezogenen Aktualisierungen und Sicherheitsfragen.

viastore fordert den benannten Hauptbenutzer regelmäßig auf, zu bestätigen, dass alle Benutzerkonten nur aktiven Mitarbeitern zugeordnet sind. Nicht bestätigte Benutzerkonten werden automatisch deaktiviert.

4.2 Anforderungen an die Informationssicherheit von Drittparteien

Bevor eine Geschäftsbeziehung eingegangen wird, muss eine Klassifizierung der Informationssicherheit von Dritten (TPIS) durchgeführt werden (siehe Anhang - Klassifizierung der Informationssicherheit von Dritten (TPIS)). Diese Bewertung bildet die Grundlage für einen risikobasierten Ansatz, der die zentralen Sicherheitsgrundsätze der Vertraulichkeit, Integrität und Verfügbarkeit berücksichtigt. Auf der Grundlage der Ergebnisse dieser Risikoanalyse müssen vertragliche Mindestsicherheitsanforderungen festgelegt werden, um sicherzustellen, dass in allen Vereinbarungen und Verträgen ein angemessenes Schutzniveau festgelegt wird.

Für Partner, die als risikoreich eingestuft werden, einen niedrigen Reifegrad in der Informationssicherheit aufweisen oder bei denen es vor kurzem zu einem Cybervorfall gekommen ist, kann dies Audits aus der Ferne oder vor Ort beinhalten, um die Umsetzung der erforderlichen Kontrollen zu überprüfen.

Diese Maßnahmen tragen dazu bei, die Sicherheits- und Lieferkettenrisiken für viastore und seine Kunden zu reduzieren, und sorgen für eine größere Widerstandsfähigkeit und Vertrauen in die Partnerschaften von viastore.

4.3 Aufrechterhaltung eines Informationssicherheitsmanagementsystems (ISMS)

Nachweis der Implementierung eines ISMS, das der ISO/IEC 27001 oder einer gleichwertigen Norm entspricht.

Dies schließt die Einhaltung von NIS2 ein.

4.4 Hintergrundüberprüfungen und NDA

Sicherstellen, dass die an der Erbringung von Dienstleistungen beteiligten Mitarbeiter überprüft wurden und Vertraulichkeits- und Sicherheitsvereinbarungen unterzeichnet haben.

Die Sicherheitsvereinbarung muss mindestens die Vertraulichkeit, die ordnungsgemäße Nutzung von IT-Ressourcen, die Zugriffsverantwortung, die Meldung von Vorfällen, den Umgang mit Daten, die Einhaltung von Richtlinien und die Verpflichtungen nach Beendigung des Arbeitsverhältnisses festlegen.

4.5 Zugangsverwaltung

Die in diesem Abschnitt 3.4 dargelegten Anforderungen gelten für alle Konten, die an der Erbringung von Dienstleistungen für viastore oder seine Kunden beteiligt sind.

- Sicherstellen, dass der Zugang zu Systemen und Daten nach dem Prinzip der geringsten Berechtigung und der Notwendigkeit des Wissens erfolgt.

- Verwenden Sie eine mehrstufige Authentifizierung (MFA) für den Zugang.
- Führen Sie aktuelle Zugriffsprotokolle und stellen Sie sicher, dass der Zugriff bei Rollenänderungen oder Vertragsbeendigung rechtzeitig widerrufen wird.
- Gemeinsame Konten sind nicht zulässig.

4.6 Änderungs- und Konfigurationsmanagement

- Alle Änderungen an Systemen müssen einem dokumentierten und genehmigten Änderungskontrollprozess folgen.
- Alle Konfigurationen müssen versionskontrolliert und überprüfbar sein.
- Trennung der Umgebungen:
  - Entwicklungs-, Test- und Produktionsumgebungen müssen strikt voneinander getrennt werden.
  - In Testumgebungen dürfen keine echten Produktionsdaten verwendet werden, es sei denn, sie sind ausdrücklich genehmigt und geschützt.

4.7 Übereinstimmung mit der Vertraulichkeitsrichtlinie von viastore

Der Umgang mit vertraulichen Daten muss streng nach der Vertraulichkeits- und Kennzeichnungsrichtlinie von **viastore** erfolgen. Dazu gehören die ordnungsgemäße Klassifizierung, die Kennzeichnung gemäß dem Datenklassifizierungsschema von **viastore** und Zugriffskontrollmaßnahmen, um eine unbefugte Offenlegung oder missbräuchliche Verwendung zu verhindern.

4.8 Sichere Handhabung und Austausch vertraulicher Daten

Vertrauliche Daten müssen so gehandhabt und ausgetauscht werden, dass ihre Vertraulichkeit und Integrität stets gewährleistet sind. Vertrauliches Material darf nur in verschlüsselter Form übertragen und gespeichert werden. Die CIA-Triade – Vertraulichkeit, Integrität und Verfügbarkeit – muss jederzeit gewahrt bleiben.

Die Verschlüsselung vertraulicher oder personenbezogener Daten während der Übertragung und im Ruhezustand muss den aktuellen Industriestandards entsprechen (z. B. AES-256, TLS 1.2+).

4.9 Schwachstellen- und Patch-Management

- Überwachung auf CVEs, die das Produkt oder seine Abhängigkeiten betreffen.
- Anwendung von Sicherheits-Patches innerhalb von 14 Tagen nach Veröffentlichung für kritische Schwachstellen.
- Durchführung regelmäßiger Schwachstellenbewertungen und Bereitstellung von Berichten auf Anfrage.

4.10 Sicherer Update-Mechanismus

- Sicherstellen, dass Aktualisierungen authentifiziert, integritätsgeschützt und nachvollziehbar sind.
- Sicherstellen, dass alle verwendeten Skripte, Dienstprogramme und Programme authentifiziert, integritätsgeschützt und nachvollziehbar sind.

4.11 Erkennung von und Reaktion auf Vorfälle

- Fähigkeiten zur Reaktion auf Vorfälle aufrechterhalten.
- Benachrichtigung von viastore über alle Sicherheitsvorfälle und Datenverletzungen innerhalb von 24 Stunden (alert@viastore.com).
- Bereitstellung von Berichten über Vorfälle und Teilnahme an koordinierten Reaktionen, falls erforderlich.

5. Anforderungen an den Datenschutz

Partner müssen:

5.1 GDPR sicherstellen

- Personenbezogene Daten in Übereinstimmung mit der GDPR und den einschlägigen nationalen Datenschutzgesetzen verarbeiten.
- die Rechte der betroffenen Personen unterstützen (Auskunft, Berichtigung, Löschung usw.).

5.2 Datenminimierung und Zweckbeschränkung

- Erfassen und verarbeiten Sie nur die Daten, die für die Erfüllung des Vertrags erforderlich sind.

5.3 Unterauftragsverarbeitung

- Holen Sie vor der Beauftragung von Unterauftragsverarbeitern die vorherige schriftliche Zustimmung ein.
- Sicherstellen, dass Unterauftragsverarbeiter dieselben Sicherheits- und Datenschutzverpflichtungen erfüllen.

5.4 Standort der Daten

- Informieren Sie viastore über die Speicherorte der Daten.
- Speichern und verarbeiten Sie die Daten innerhalb der EU oder in Ländern mit einem angemessenen Schutzniveau.

5.5 Löschung und Rückgabe von Daten

- Rückgabe oder sichere Löschung aller Daten bei Vertragsende gemäß den Aufbewahrungsrichtlinien des Unternehmens.
- Löschen Sie alle Konfigurationsdateien, Skripte, API-Schlüssel, Anmeldeinformationen usw. nach Beendigung des Projekts oder des Auftrags.

6. Prüfung und Einhaltung

- Die Organisation behält sich das Recht vor, die Einhaltung dieser Richtlinie durch die Partner zu überprüfen.
- Die Partner müssen bei den Prüfungen kooperieren und auf Anfrage Nachweise für die Einhaltung dieser Richtlinie vorlegen. Dazu gehört auch der jährliche Fragebogen zur Selbsteinschätzung der Partner von viastore.
- Die Nichteinhaltung kann zur Vertragskündigung oder zu rechtlichen Schritten führen.
- Auditrechte müssen vertraglich in der Hauptvereinbarung festgelegt werden.

7. Bereitstellung von Informations- und Kommunikationstechnologie (IKT) und integrierten Dienstleistungen

Wenn der Partner Produkte oder Dienstleistungen der Informations- und Kommunikationstechnologie (IKT) liefert, die in die Umgebung von **viastore** oder des Kunden integriert sind:

7.1 Einhaltung der CRA/IEC62443-Verpflichtungen

- Erfüllung der CRA/IEC62443-Anforderungen für die sichere Produktentwicklung, den Umgang mit Sicherheitslücken und die Transparenz der Lieferkette.
- Geeignete Kontrollen müssen auf dem Ergebnis einer detaillierten Risiko- und Bedrohungsbewertung basieren. Die endgültige Genehmigung der Risikoakzeptanz obliegt dem CISO von **viastore**.

7.2 Sicherheit durch Design und Standard

- Es ist sicherzustellen, dass die Produkte standardmäßig sichere Konfigurationen enthalten und eine Dokumentation der Sicherheitsmerkmale bereitgestellt wird.

7.3 Software-Stückliste (SBOM)

- Stellen Sie auf Anfrage eine aktuelle und genaue SBOM zur Verfügung.
- Informieren Sie die Organisation über alle bekannten Sicherheitslücken in den verwendeten Komponenten.

7.4 Unterstützung und Aktualisierungen

- Verpflichtet sich zu einem festgelegten Support- und Aktualisierungszeitraum. Der Anbieter muss die Verfügbarkeit von Updates und Sicherheitsverbesserungen für einen Zeitraum von mindestens fünf Jahren garantieren.
- **viastore** im Voraus über das End-of-Life (EOL) zu informieren.

8. Anforderungen an die Softwareentwicklung

Die an der Code-Entwicklung beteiligten Partner müssen:

8.1 einen sicheren Entwicklungslebenszyklus (SDLC) anwenden

- einen formalen SDLC-Prozess implementieren, der Bedrohungsmodellierung, Risikobewertung, sicheres Design, sichere Kodierung und Peer Code Reviews umfasst.

8.2 Sichere Entwicklungspraktiken

- Befolgen Sie die Standards für sichere Kodierung (z. B. OWASP).
- Durchführung von Code-Reviews und Sicherheitstests (SAST, DAST) vor dem Einsatz von Softwarekomponenten, die in die Systeme der Organisation integriert werden sollen.

8.3 Befolgen Sie die Standards für sichere Kodierung

- Befolgen Sie Standards wie die OWASP Top 10, CWE und SANS-Richtlinien.
- Vermeiden Sie die Verwendung von veralteten oder unsicheren Bibliotheken oder Funktionen.

8.4 Code-Prüfung

- Führen Sie statische und dynamische Sicherheitstests (SAST & DAST) durch.
- Bereitstellung der Testergebnisse und Behebung von Schwachstellen vor der Auslieferung.

8.5 Versionskontrolle und Rückverfolgbarkeit

- Verwenden Sie Versionskontrollsysteme (z. B. Git) mit ordnungsgemäßer Commit-Dokumentation.
- Gewährleisten Sie eine vollständige Rückverfolgbarkeit zwischen Anforderungen, Codeänderungen und Implementierungen.

8.6 Software-Stückliste (SBOM)

- Stellen Sie eine vollständige und genaue SBOM für jedes Produkt zur Verfügung.

- Deklarieren Sie bekannte Schwachstellen und Abhängigkeiten, die in der Software verwendet werden.

8.7 Keine Hintertüren oder unzulässige Logik

- Die Partner dürfen keine versteckte Logik, fest kodierte Anmeldeinformationen oder Telemetrie-Mechanismen implementieren, es sei denn, dies wurde ausdrücklich genehmigt.

9. Geistiges Eigentum und Quellcode-Eigentum

Sofern in der Hauptvereinbarung nichts anderes vorgesehen ist, gilt Folgendes:

- Alle entwickelten Codes, Skripte und Konfigurationen sind das geistige Eigentum von **viastore**, sofern nicht anders angegeben.
- Der Partner darf Code oder Konfigurationen nicht kundenübergreifend wiederverwenden, es sei denn, es handelt sich um Open Source oder es ist ausdrücklich erlaubt.

10. Einhaltung des EU-Datenschutzgesetzes

Alle Partner und Lieferanten müssen Daten im Auftrag von viastore oder einem Kunden von viastore in voller Übereinstimmung mit dem EU-Datenschutzgesetz behandeln und dabei Transparenz, Interoperabilität und einen sicheren Datenaustausch gewährleisten. Dies umfasst alle Produkte oder Dienstleistungen, die im Rahmen eines Kundenprojekts oder einer Installation geliefert werden.

10.1 Anforderungen

- **Datenzugriff und -portabilität:** Partner und Lieferanten müssen auf Anfrage von viastore oder dem Kunden einen sicheren Echtzeit-Zugriff auf die von Produkten/Dienstleistungen generierten Daten in maschinenlesbaren Formaten ermöglichen.
- **Governance der Datenweitergabe:** Partner und Lieferanten müssen technische und organisatorische Maßnahmen ergreifen, um eine rechtmäßige, faire und diskriminierungsfreie Weitergabe von Daten zu gewährleisten.
- **Sicherheit und Vertraulichkeit:** Alle gemeinsam genutzten Daten müssen durch Verschlüsselung, Zugriffskontrollen und Prüfprotokolle geschützt werden. Lieferanten müssen die Verpflichtungen der DSGVO und NIS2 einhalten.
- **Offenlegung von Unterauftragsverarbeitern:** Partner und Lieferanten müssen alle Unterauftragsverarbeiter offenlegen und sicherstellen, dass diese gleichwertige Compliance-Standards erfüllen.
- **Löschung und Rückgabe von Daten:** Nach Beendigung des Vertrags müssen Partner und Lieferanten alle Unternehmensdaten sicher löschen oder zurückgeben.

11. Einhaltung des EU-Künstlicher-Intelligenz-Gesetzes (AI Act)

Alle Partner und Lieferanten müssen KI-Systeme in voller Übereinstimmung mit dem EU-KI-Gesetz und den ethischen Standards von viastore entwickeln, einsetzen oder integrieren. Dies gilt für alle Produkte oder Dienstleistungen, die im Rahmen eines Kundenprojekts oder einer Installation geliefert werden.

11.1 Requirements

- **Risikoklassifizierung:** Partner und Lieferanten müssen gemäß Artikel 6 des EU-KI-Gesetzes das Risikoniveau jedes KI-Systems bewerten und dokumentieren (verboten, risikoreich, begrenzt, minimal).
- **Risikoreiche KI-Systeme:** Müssen eine CE-Kennzeichnung, Risikoregister und Mechanismen zur menschlichen Überwachung enthalten und in der EU-Datenbank registriert sein.
- **Transparenzpflichten:** Partner und Lieferanten müssen synthetische Inhalte klar kennzeichnen, die Verwendung von KI gegenüber den Nutzern offenlegen und Unterlagen zu Trainingsdaten und Modellverhalten bereitstellen.
- **Protokollierung von Vorfällen:** Partner und Lieferanten müssen schwerwiegende Vorfälle oder Fehlfunktionen im Zusammenhang mit KI-Systemen protokollieren und melden.
- **Ethische Nutzung:** KI-Systeme dürfen nicht für Social Scoring, biometrische Kategorisierung oder manipulatives Verhalten verwendet werden, es sei denn, dies ist ausdrücklich genehmigt.
- **Sicherheit durch Design:** KI-Systeme müssen mit integrierten Sicherheitskontrollen, Rückverfolgbarkeit und Erklärbarkeit entwickelt werden.
- **KI-Tools von Drittanbietern:** Partner und Lieferanten, die KI von Drittanbietern verwenden, müssen sicherstellen, dass diese Tools mit dem EU-KI-Gesetz und der DSGVO konform sind.

11.2 Richtlinie zum Eigentum und zur Nutzung von KI-generierten Modellen und Daten

Alle für **viastore** und die Kunden von **viastore** entwickelten KI-Modelle – einschließlich, aber nicht beschränkt auf große Sprachmodelle (LLMs) – sowie alle von diesen Modellen generierten Daten (Ausgaben, Vorhersagen, Antworten usw.) sind das ausschließliche geistige Eigentum von **viastore**. Die Verwendung interner oder vertraulicher Daten zum Zwecke des Trainings, der Feinabstimmung oder anderweitigen Verbesserung von KI-Systemen muss ausdrücklich schriftlich durch die Geschäftsführung von **viastore** oder den CISO genehmigt werden. Die unbefugte Nutzung, Weitergabe oder externe Offenlegung solcher Modelle oder ihrer Ergebnisse ist untersagt.

12. Schulung und Sensibilisierung

Der Partner stellt sicher, dass alle an der Leistungserbringung beteiligten Mitarbeiter und Auftragnehmer angemessen und regelmäßig in Fragen der Cybersicherheit und des Datenschutzes geschult werden.

Dazu gehören auch Schulungen zu den Verfahren und Richtlinien von **viastore**. Die Inhalte der Schulungen werden von **viastore** ausgewählt.

13. Anerkennung der Richtlinie

Diese Richtlinie wird durch Verweis in den Hauptvertrag aufgenommen. Die Partner müssen sie anerkennen und ihren Bedingungen zustimmen, bevor sie mit der Datenverarbeitung oder der Erbringung von Dienstleistungen beginnen.

Jeder Partner muss die **viastore** "Vereinbarung über die Nutzung der **viastore** IT-Einrichtungen" (1.034) unterzeichnen.

Jeder Mitarbeiter, der Zugang hat, muss die Kenntnisnahme durch Unterzeichnung der "Erklärung zur Nutzung der **viastore**-IT-Einrichtungen für externe Nutzer" (1.034-1) bestätigen.

14. Anhang - Sicherheitsklassifizierung von Informationen Dritter (TPIS)

14.1 Zielsetzung

Ziel des TPIS-Prozesses ist es, Partner auf der Grundlage des Informationssicherheitsrisikos, das sie für **viastore** oder **viastore**-Kunden darstellen, zu bewerten und zu klassifizieren. Dies gewährleistet verhältnismäßige und risikogerechte Sicherheitskontrollen während des gesamten Lebenszyklus des Produkts oder der Dienstleistung.

14.2 Geltungsbereich

Gilt für alle Partner, die:

- Produkte oder Dienstleistungen mit digitalen Komponenten liefern;
- auf **viastore**- oder Kundendaten zugreifen, diese verarbeiten, übertragen oder speichern oder
- kritisch für die Lieferkette oder die Erfüllung vertraglicher Verpflichtungen sind.

14.3 Klassifizierungsstufen

Stufe	Beschreibung	Beispiele	Typische erforderliche Kontrollen
Hoch	Erhebliche Auswirkungen auf den Betrieb, die Daten oder die Einhaltung von Vorschriften, wenn diese gefährdet sind	Cloud-Anbieter, Software-Integratoren, Hosting-Anbieter	Vollständiger Sicherheitsfragebogen, ISO 27001 oder gleichwertiger Nachweis, Auditrechte, Audit vor Ort
Mittel	Mäßiger Zugriff auf Systeme oder Daten oder wichtige betriebliche Abhängigkeiten	Fernservice-Techniker, Logistiksoftware-Partner	Selbsteinschätzung der Sicherheit, Vertraulichkeitsvereinbarung, Vertragsklauseln
Gering	Minimaler oder kein digitaler Zugang; begrenzte betriebliche Abhängigkeit	Hardware-Lieferanten ohne Software, Anbieter von Büroausstattung	Einfache NDA, Bestätigung des Sicherheitsbewusstseins

14.4 Berücksichtigte Risikofaktoren

- Zugang zu **viastore**- oder Kundendaten (Art, Umfang, Sensibilität)
- Zugang zu **viastore**-Systemen oder -Netzwerken
- Kritische Bedeutung für die Betriebskontinuität oder die Lieferkette
- Einbeziehung digitaler Komponenten (Firmware, Konnektivität, APIs)

- Frühere Sicherheitsvorfälle oder Reifegradlücken
- Hosting-Modell (vor Ort, hybrid, Cloud)

14.5 Klassifizierungsprozess

1. Auslösung: Ausgelöst vor Vertragsunterzeichnung oder Onboarding.
2. Datenerhebung: Über Cloud- und Lieferantenfragebögen und technische Dokumentation.
3. Risikobewertung: Wird von Informationssicherheit und Beschaffung gemeinsam durchgeführt.
4. Zuweisung der Klassifizierung: Auf der Grundlage der vordefinierten Kriterien oben.
5. Dokumentation: Aufzeichnung im Risikoregister des Lieferanten und im ERP-/Beschaffungstool.
6. Häufigkeit der Überprüfung: Mindestens alle 24 Monate oder nach wesentlichen Änderungen.

14.6 Durchsetzung und Eskalation

- Bei Lieferanten mit hohem Risiko kann es zu Vor-Ort-Audits, zusätzlichen Vertragsklauseln oder Verzögerungen beim Onboarding kommen, bis die Sicherheitslücken behoben sind.
- Die endgültige Entscheidung über die Einstufung und die Genehmigung des Risikominderungsplans obliegt dem CISO von viastore.

14.7 Vorteile

- Passt die Kontrollen von Drittanbietern an das Geschäftsrisiko an.
- Erhöht die Sicherheit und Widerstandsfähigkeit der Lieferkette.
- Unterstützt die Einhaltung von ISO 27001, NIS2, anderen Informationssicherheits- und Datenschutzgesetzen und Kundenanforderungen.