Leitlinie zum Datenschutz- und Informationssicherheitsmanagement

Gewerbepark Meißen 17
32423 Minden

Stand: 06.09.2019
Rev. 01

Inhalt

1. Geltungsbereich

Diese Leitlinie zum Datenschutz- und Informationssicherheitsmanagement (DISM) gilt für Paletti und verpflichtet alle Mitarbeiter zur Beachtung und Einhaltung an allen Standorten.

2. Ziele

Paletti (auch Unternehmen) verarbeitet eine Vielzahl von (auch personenbezogenen) Daten und Informationen, um ihre Aufgaben und Pflichten gegenüber Mitarbeitern, Kunden, Vertragspartnern, Dienstleistern, öffentlichen Stellen und sonstigen Dritten zu erfüllen.

Die Geschäftsführung von Paletti verabschiedet daher nachfolgende Leitlinie zum Datenschutz- und Informationssicherheitsmanagement, um die Strategie, die Organisation und die Ziele des Datenschutzes und der Informationssicherheit im Unternehmen in übersichtlicher Form darzustellen sowie die Einhaltung der Anforderungen zu Datenschutz und Informationssicherheit zu gewährleisten.

Ziel der Informationssicherheit ist es Informationen (Daten, Technologien, Systeme, Know-How, sowie weitere Unternehmenswerte der Informationssicherheit) gegen den Verlust der Vertraulichkeit, Verfügbarkeit und Integrität zu schützen und somit die Kundenzufriedenheit und die Wettbewerbsfähigkeit von Paletti nachhaltig sicherzustellen.

3. Anforderungen

Ziel dieser Leitlinie ist es, den Datenschutz und die Informationssicherheit im Unternehmen zu gewährleisten, um die internen und externen Anforderungen zu erfüllen. Die Anforderungen setzen sich wie folgt zusammen:

3.1 Interne Anforderungen

Einhaltung des internen Qualitätsmanagementsystems inklusive aller Richtlinien und Vorgaben enthalten im QM-System.

Vermeidung von Informationssicherheits- und Datenschutzvorfällen mit direkten und indirekten finanziellen Auswirkungen auf die Gesellschaften von Paletti.

3.2 externe Anforderungen

3.2.1 gesetzliche Anforderungen

Die gesetzlichen Anforderungen mit Einfluss auf das DISM stellen die DS-GVO und das Bundesdatenschutzgesetz (BDSG).

3.2.2 weitere externe Anforderungen

Ziel des DISM bei Paletti ist es, die Wünsche und Anforderungen bezüglich des Datenschutzes und der Informationssicherheit der Kunden der jeweiligen Aufträge zu erfüllen.

3.2.3 normative Anforderungen

Nach VDA ISA Version 4.1.1

4. Sanktionen

Ein Verstoß gegen diese Leitlinie zum Datenschutz- und Informationssicherheitsmanagement sowie die Nichtbeachtung der hierin geregelten Vorgaben kann eine arbeitsvertragliche Pflichtverletzung und/oder einen Verstoß gegen geltendes Recht darstellen und entsprechend durch die Geschäftsführung sanktioniert werden.

5. Datenschutz- und Informationssicherheitsmanagement

5.1 Notwendigkeit von Datenschutz und Informationssicherheit

Die im Unternehmen zu verarbeitenden und zu nutzenden Daten (Informationen) und die eingesetzten Technologien der Verarbeitung stellen wichtige Instrumente zur Sicherung des Unternehmenserfolges dar. Sie müssen aus diesen Gründen vor Verlust und zufälliger Zerstörung (Verfügbarkeit), unbefugter Veränderung (Integrität) sowie unbefugter Nutzung und unbefugtem Zugang (Vertraulichkeit) geschützt werden. Damit sind Datenschutz und Informationssicherheit auch ein wesentlicher Bestandteil des allgemeinen Qualitäts- und Risikomanagements.

Um diese Ziele zu erreichen, müssen die unter Kapitel 3 genannten Anforderungen eingehalten werden.

Nicht zuletzt kommt es aber auch darauf an, dass sich alle Mitarbeiter der mit der Datenverarbeitung und der Benutzung der IT-Systeme und Telekommunikationstechnologien verbundenen Risiken bewusst sind und mit Daten und IT-Systemen mit der erforderlichen Vorsicht und Sorgfalt umgehen. Aus diesem Grund werden alle Mitarbeiter, in geeigneter Weise im Datenschutz und der Informationssicherheit geschult und zur Einhaltung der Vorgaben aus den entsprechenden Richtlinien verpflichtet.

5.2 Managementsystem für Datenschutz und Informationssicherheit

Um im Unternehmen einen dauerhaften Prozess zu etablieren, welcher die Planung, Umsetzung, Überprüfung und Verbesserung des Datenschutzes und der Informationssicherheit gewährleistet, wurde dieses Managementsystem in Form eines kontinuierlichen Verbesserungsprozesses (KVP) eingeführt.

Es wird regelmäßig weiterentwickelt und durch die in Kapitel 6 beschriebenen Verantwortlichen an die Bedürfnisse des Unternehmens, der Gesetze, der technischen und wirtschaftlichen Entwicklung und die Anforderungen des TISAX-Standards angepasst.

5.3 Aufbau des Regelwerks

Den Risiken durch Verstöße gegen die definierten Anforderungen, aber auch dem Verlust von geistigem Eigentum, Geschäftsgeheimnissen und Imageschäden soll durch entsprechende Maßnahmen proaktiv begegnet werden. Alle Mitarbeiter sind daher verpflichtet, sich an das entsprechende Regelwerk zu halten.

Den allgemeinen Rahmen bildet diese Leitlinie zum Datenschutz- und Informationssicherheitsmanagement, welche durch verschiedene Richtlinien ergänzt wird.

Damit die Regelungen überschaubar bleiben, sind diese in verschiedene Einzelrichtlinien aufgeteilt. Hierbei ist im Kapitel 1 der jeweiligen Richtlinien geregelt, für welche Personengruppen die entsprechende Richtlinie gilt. In jeder Richtlinie können Verweise auf andere Richtlinien oder Dokumente erfolgen, welche ebenfalls zu berücksichtigen sind. Diese werden grundsätzlich so dargestellt: „*Dokumentenname kursiv*".

6. Verantwortlichkeiten

Namen und Aufgaben der definierten Personen sind der Anlage „*Aufgaben und Personen*" zu entnehmen.

6.1 Geschäftsleitung

Die Geschäftsleitung übernimmt die Gesamtverantwortung für die Informationssicherheit und den Datenschutz im Unternehmen. Sie setzt die Richtlinien und Arbeitsanweisungen in Kraft.

6.2 Datenschutzbeauftragter (DSB)

Paletti hat einen Datenschutzbeauftragten (DSB) bestellt.

Im Bereich der Verarbeitung von personenbezogenen Daten ist Sorge dafür zu tragen, dass eine frühzeitige Einbindung des Datenschutzbeauftragten bei der Planung und Einführung von neuen Prozessen, in deren Zusammenhang auch personenbezogenen Daten verarbeitet werden, erfolgt. Gleiches gilt für Änderungen an bestehenden Prozessen.

6.3 Informationssicherheitsbeauftragter (ISB)

Zur Erreichung der Ziele des DISMS, benennt die Geschäftsleitung einen Informationssicherheitsbeauftragten (ISB).

Der Informationssicherheitsbeauftragte berät die Geschäftsleitung bei der Planung und Umsetzung der Informationssicherheit im Unternehmen. Er berichtet in seiner Funktion anlassbezogen, mindestens jedoch einmal jährlich, unmittelbar an die Geschäftsleitung.

Der Informationssicherheitsbeauftragte hat die Aufgabe der Initiierung, Planung, Umsetzung und Steuerung des Informationssicherheitsprozesses (ISP) im Unternehmen. Er ist zentraler Ansprechpartner für Informationssicherheit im Unternehmen.

Dem Informationssicherheitsbeauftragten werden von der Geschäftsleitung die notwendigen finanziellen und zeitlichen Ressourcen zur Verfügung gestellt, um sich zur Wahrnehmung der zuvor genannten Aufgaben entsprechend weiterzubilden und zu informieren.

Der Informationssicherheitsbeauftragte ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen.

6.4 Datenschutz- und Informationssicherheitsteam (DIST)

Es wird ein Datenschutz- und Informationssicherheitsteam (DIST) gebildet, welches die Planung, Umsetzung und Evaluierung von Datenschutz und Informationssicherheit im Unternehmen begleitet.

Das DIST unterstützt den DSB und ISB bei der Planung, Koordinierung und Umsetzung von Datenschutz und Informationssicherheit im Unternehmen. Dieses Team trifft sich in regelmäßigen Abständen, um den Prozess der kontinuierlichen Verbesserung zu gewährleisten.

6.5 IT-Administratoren

Die IT-Administratoren führen insbesondere die technischen Maßnahmen durch und tragen durch Verbesserungsvorschläge zur Optimierung der Informationssicherheit bei.

6.6 Vorgesetzte

Vorgesetzte tragen durch ihr Verhalten zur Gewährleistung von Datenschutz und Informationssicherheit bei.

Vorgesetzte mit Personalverantwortung haben die Aufgabe sicherzustellen, dass die getroffenen technischen und organisatorischen Maßnahmen zu Datenschutz und Informationssicherheit in Bezug auf die in ihrem Verantwortungsbereich tätigen Personen umgesetzt werden.

6.7 Mitarbeiter

Jeder Mitarbeiter trägt durch sein Verhalten zur Gewährleistung von Datenschutz und Informationssicherheit bei.

Alle Mitarbeiter sind verpflichtet, diese Leitlinie und die Richtlinien zum Datenschutz und der Informationssicherheit für Mitarbeiter zu beachten und einzuhalten.

Um Datenschutz und Informationssicherheit im Unternehmen zu gewährleisten, ist jeder Mitarbeiter verpflichtet, Störungen, Datenschutz- und Sicherheitsvorfälle sowie Notfälle im Bereich der Informationssicherheit und des Datenschutzes unverzüglich auf den in der Richtlinie zum Umgang mit Datenschutz- und Sicherheitsvorfällen definierten Wegen zu melden.

6.8 Lieferanten und Dienstleister

Lieferanten, externe Dienstleister und sonstige Auftragnehmer sind ausschließlich gemäß der Richtlinie für Auftragsverarbeitung und Sicherheit der Dienstleister zu beauftragen.

7. Dokumentsteuerung

Diese Leitlinie wurde am 06.09.2019 von der Geschäftsleitung beschlossen und den Mitarbeitern sowie Dienstleistern bekannt gegeben.

Sie wird mindestens jährlich von der Geschäftsleitung auf Aktualität geprüft und bei Bedarf angepasst, beschlossen und erneut bekannt gegeben.

Dokumentenhistorie

Version	Datum	Beschreibung	Name
01	21.08.2019	Initialisierung, Festlegung von Zielen, Verantwortlichkeiten, Ressourcen	DIST