Leitlinie zum Datenschutz und Informationssicherheit

1. Einleitung

Die **The Nunatak Group GmbH** verabschiedet hiermit die Leitlinie zum Datenschutz und Informationssicherheit in unserem Unternehmen.

Als Unternehmen verarbeiten wir eine Vielzahl von (personenbezogenen) Daten, um unsere Aufgaben und Pflichten gegenüber unseren Kunden, Vertragspartnern, Dienstleistern und sonstigen Stakeholdern zu erfüllen.

Dabei verarbeiten wir Daten mit unterschiedlichem Schutzbedarf. Die Sicherheit der Informationsverarbeitung und der Schutz von personenbezogenen Daten spielen eine wesentliche Rolle in unserem Unternehmen. Diese Leitlinie soll die Strategie, die Organisation und Ziele von Datenschutz und Informationssicherheit in unserem Unternehmen in übersichtlicher Form darstellen.

2. Geltungsbereich

Diese Leitlinie verpflichtet alle Beschäftigten der **The Nunatak Group GmbH** zur Einhaltung der hier festgelegten Pflichten.

Mitarbeitende und externe Geschäftspartner werden bei Bedarf über für sie relevante Änderungen von **The Nunatak Group GmbH** informiert.

3. Ziele

Cybersecurity und Produktsicherheit

Die **The Nunatak Group GmbH** verpflichtet sich, die Sicherheit ihrer Dienstleistungen zu gewährleisten, die potenziellen Risiken von Cyber-Angriffen ausgesetzt sein können. Das Unternehmen hat angemessene technische und organisatorische Maßnahmen ergriffen, um die Resilienz seiner Systeme, Netzwerke und Daten zu erhöhen und die Auswirkungen von Sicherheitsvorfällen zu minimieren. Das Unternehmen stellt sicher, dass seine Dienstleistungen in Übereinstimmung mit den geltenden rechtlichen Anforderungen und Standards für Cybersecurity entwickelt und bereitgestellt werden. Das Unternehmen fördert zudem die sichere Entwicklung seiner Leistungen, indem es Sicherheitsaspekte in allen Phasen des Beratungszyklus berücksichtigt.

Beschäftigte

Die **The Nunatak Group GmbH** verpflichtet sich, das Bewusstsein und die Kompetenz ihrer Beschäftigten für Datenschutz und Informationssicherheit zu erhöhen. Das Unternehmen führt regelmäßige Schulungen und Sensibilisierungsmaßnahmen durch, um die Beschäftigten über die möglichen Bedrohungen und Schutzmaßnahmen zu informieren. Das Unternehmen fördert eine Kultur der Verantwortung und des Vertrauens, in der die Beschäftigten aktiv zur Verbesserung der Datenschutz und Informationssicherheitspraktiken beitragen.

Vielschichtigkeit

Die **The Nunatak Group GmbH** erkennt an, dass Datenschutz und Informationssicherheit vielschichtige und dynamische Herausforderungen darstellen, die sowohl physische als auch digitale Aspekte umfassen. Das Unternehmen verfolgt einen ganzheitlichen und risikobasierten Ansatz, um die verschiedenen Dimensionen der Sicherheit zu adressieren, wie z. B. Hardware, Software, Netzwerke, Daten, Personen, Prozesse und Organisation. Das Unternehmen überwacht und bewertet die sich ständig ändernde Sicherheitslandschaft und die bestehenden und aufkommenden Bedrohungen und Schwachstellen.

4. Organisation von Datenschutz und Informationssicherheit

Zur Erreichung der Ziele dieser Richtlinie wurde ein **Datenschutzbeauftragter** von der Unternehmensleitung benannt. Der Datenschutzbeauftragte berät die Geschäftsführung zusätzlich bei der Planung und Umsetzung der **Informationssicherheit** im Unternehmen. Er berichtet in seiner Funktion anlassbezogen, mindestens jedoch einmal jährlich, unmittelbar an die Geschäftsführung.

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

Im Bereich der Verarbeitung von personenbezogenen Daten ist Sorge dafür zu tragen, dass eine frühe 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. Gleiches gilt für Projekte und Changes, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen.

Im Unternehmen existiert für die Bereiche Informationssicherheit und Datenschutz ein **Managementsystem**. Hierfür ist im Unternehmen ein Prozess der kontinuierlichen Verbesserung mit dem Ziel implementiert, die einzelnen Maßnahmen in den Bereichen so zu koordinieren, dass die Ziele dieser Leitlinie erreicht werden.

Es ist ein **Datenschutz- und Informationssicherheitsteam („Datenschutzteam“ - DST)** gebildet, dass die Planung, Umsetzung und Evaluierung von Datenschutz und Informationssicherheit im Unternehmen begleitet und unterstützt. Das DST plant die für die Umsetzung der Ziele dieser Leitlinie erforderlichen Richtlinien, stimmt diese mit der Geschäftsführung ab, überprüft regelmäßig ihre Wirksamkeit und nimmt erforderlichenfalls Anpassungen vor. Für den Fall, dass das DST in Fragen der Planung, Umsetzung, Evaluierung oder Anpassung von Richtlinien oder bei der Beurteilung von Sach- oder Rechtsfragen uneinig ist, wird das DST dies der Geschäftsführung vortragen. Die Geschäftsführung wird dann entscheiden und erforderlichenfalls Maßnahmen veranlassen.

Unternehmensrichtlinien werden von der Geschäftsführung verbindlich gemacht, so dass sie von den jeweiligen Adressaten der Richtlinie einzuhalten sind und Verstöße ggf. sanktioniert werden können.

5. Maßnahmen

Ein **Risikomanagement** ist etabliert, um die Sicherheit der Daten und Informationen gewährleisten zu können. Das bedeutet, dass das DST regelmäßig Risikoanalysen durchführt, um die potenziellen Bedrohungen und Schwachstellen für die Vertraulichkeit, Integrität und Verfügbarkeit zu identifizieren und zu bewerten. Basierend auf den Ergebnissen der Risikoanalysen wird das DST geeignete Maßnahmen zur Reduzierung oder Beseitigung der Risiken festlegen und umsetzen. Die Maßnahmen werden nach dem Grundsatz der Erforderlichkeit und Verhältnismäßigkeit ausgewählt, d. h. sie sollen angemessen, wirksam und effizient sein, ohne unverhältnismäßige Nachteile oder Kosten zu verursachen. Der Informationssicherheitsbeauftragte überprüft die Wirksamkeit der Maßnahmen und überwacht diese, ob sie die festgelegten Ziele erreichen und ob sie an veränderte Umstände oder neue Anforderungen angepasst werden müssen.

Die Maßnahmen zur Umsetzung dieser Leitlinien können in Form von technischen und organisatorischen Maßnahmen erfolgen. Dazu gehören auch Richtlinien, betriebliche Regelungen oder betriebliche Anweisungen. Diese sind von den Beschäftigten zu befolgen.

6. Verantwortlichkeiten

Die **Unternehmensleitung** übernimmt die Gesamtverantwortung für die **Informationssicherheit** und den **Datenschutz** im Unternehmen.

Der **Datenschutzbeauftragte** ist Ansprechpartner für das Thema Datenschutz und Informationssicherheit im Unternehmen. Er berät, kontrolliert und unterstützt die Unternehmensleitung und Beschäftigten hinsichtlich der Verarbeitung von personenbezogenen Daten im Unternehmen. Seine Aufgaben ergeben sich aus den datenschutzrechtlichen Vorschriften (DSGVO, BDSG etc.) und zusätzlicher gesetzlicher Vorgaben (NIS2, AI-Act) im Bereich Informationssicherheit.

Das **Datenschutz- und Informationssicherheitsteam** unterstützt den Datenschutzbeauftragten 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.

Die **IT-Administration** setzt die Richtlinien und sonstigen Vorgaben zu Datenschutz und Informationssicherheit in ihrem Verantwortungsbereich um. Sie stimmt Maßnahmen, die Auswirkungen auf die Informationssicherheit haben, mit dem Informationssicherheitsbeauftragten ab. Sie führt die technischen Maßnahmen in Abstimmung mit der Unternehmensleitung durch und trägt durch Verbesserungsvorschläge zur Optimierung der Informationssicherheit bei.

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

Alle **Mitarbeitenden** tragen durch ihr Verhalten zur Gewährleistung von Datenschutz und Informationssicherheit bei. Sie sind verpflichtet, diese Leitlinie und die Richtlinien zu Datenschutz und Informationssicherheit einzuhalten. Um Datenschutz und Informationssicherheit im Unternehmen zu gewährleisten, ist jeder Mitarbeiter verpflichtet, Störungen, Sicherheitsvorfälle und Notfälle im Bereich der Informationssicherheit unverzüglich und direkt an den Datenschutzbeauftragten zu melden.

Projekt- oder Prozessverantwortliche müssen den Datenschutzbeauftragten bei allen Projekten mit Auswirkung auf die Verarbeitung personenbezogener Daten konsultieren, um sicherzustellen, dass datenschutzrechtliche Vorschriften eingehalten werden können. Ferner sind alle Projekt- oder Prozessverantwortlichen verpflichtet, den Datenschutzbeauftragten bei allen Projekten zu konsultieren, die Auswirkung auf die Informationssicherheit im Unternehmen haben.

Lieferanten, externe Dienstleister und sonstige Auftragnehmer sind durch gesonderte Vereinbarungen zu verpflichten, die sie betreffenden Vorgaben zu Datenschutz und Informationssicherheit einzuhalten, wenn diese Daten im Auftrag verarbeiten oder die Möglichkeit der Kenntnisnahme von personenbezogenen Daten oder als nicht öffentlich klassifizierte Informationen des Unternehmens haben.

7. Sanktionen

Ein Verstoß gegen diese Leitlinie kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

Für Lieferanten, externe Dienstleister und sonstige Auftragnehmer sind bei besonderen Risiken Vertragsstrafen Regelungen zu vereinbaren.