Supplier Code of Conduct

Verhaltenskodex für Lieferanten

Erstellt: 01.01.2024 durch **QMB** - Volljuristin Tamara Artinger

Vorwort:

Die REMSA Gesellschaft für RZ-Organisation EDV-Beratung Methoden-Beratung Software-Entwicklung Anwender-Schulung mbH ist bestrebt, ihre Geschäfte mit Integrität, Verantwortung und unter Berücksichtigung ethischer, sozialer und umweltfreundlicher Grundsätze zu führen. Unsere Lieferanten spielen eine wesentliche Rolle, um diese Standards aufrechtzuerhalten. Dieser **Supplier Code of Conduct** definiert die Erwartungen, die wir an unsere Lieferanten in Bezug auf rechtliche Compliance, ethische Geschäftspraktiken, soziale Verantwortung und Umweltschutz haben. Wir erwarten, dass unsere Lieferanten diesen Verhaltenskodex einhalten und sicherstellen, dass diese Grundsätze auch bei ihren eigenen Lieferanten und Unterauftragnehmern eingehalten werden.

Adresse:

REMSA Gesellschaft für RZ-Organisation EDV-Beratung Methoden-Beratung Software-Entwicklung Anwender-Schulung mbH
Lateinschulgasse 15
94469 Deggendorf

Kontakt:

Web: https://www.remsa.de/
E-Mail: Info@remsa.de
Tel.: +49 991 25031 73

Amtsgericht Deggendorf, HRB 2828
Geschäftsführer: Konrad Artinger

Inhalt:

Kapitel 1: Einführung

Die REMSA GmbH strebt danach, ethische, nachhaltige und langfristige Partnerschaften mit ihren Lieferanten aufzubauen, die auf gegenseitigem Vertrauen, Respekt und gemeinsamen Werten basieren. Dieser Supplier Code of Conduct stellt klare Erwartungen und Richtlinien für die Geschäftsbeziehung dar und definiert die Standards, die wir von allen unseren Lieferanten in Bezug auf ethische Geschäftspraktiken, soziale Verantwortung, Umweltschutz und Compliance erwarten.

1.1. Gemeinsame Verantwortung

Als Lieferant der REMSA GmbH tragen Sie eine wesentliche Verantwortung zur Sicherstellung, dass diese Standards in allen Bereichen der Geschäftsbeziehung eingehalten werden. Die Einhaltung der hier festgelegten Anforderungen ist nicht nur eine Bedingung für unsere Zusammenarbeit, sondern trägt auch dazu bei, eine bessere, gerechtere und nachhaltigere Wirtschaft zu fördern.

Wir glauben, dass Unternehmen, die ethische Standards in den Mittelpunkt ihrer Geschäftstätigkeit stellen, nicht nur langfristig erfolgreich sind, sondern auch positive Auswirkungen auf die Gesellschaft und die Umwelt haben. Wir ermutigen unsere Lieferanten, diese Grundsätze nicht nur zu akzeptieren, sondern aktiv in ihren Organisationen umzusetzen und kontinuierlich zu verbessern.

1.2. Kontinuierliche Verbesserung

Die REMSA GmbH ist bestrebt, gemeinsam mit ihren Lieferanten an der kontinuierlichen Verbesserung der Qualität, Sicherheit und Nachhaltigkeit der Produkte und Dienstleistungen zu arbeiten. Wir sehen den Supplier Code of Conduct nicht nur als statisches Dokument, sondern als dynamischen Rahmen, der sich an neue Entwicklungen in der Branche und an geänderte gesetzliche Vorgaben anpassen wird.

Unsere Lieferanten sind eingeladen, uns regelmäßig über Verbesserungen in ihren Prozessen und Praktiken zu informieren, um die Qualität der Zusammenarbeit weiter zu steigern. Innovationen und Best Practices, die zur Erfüllung oder Verbesserung der im Code genannten Standards beitragen, werden von uns aktiv unterstützt und gefördert.

1.3. Partnerschaftliche Zusammenarbeit

Die REMSA GmbH setzt auf eine partnerschaftliche Zusammenarbeit mit ihren Lieferanten. Wir sind überzeugt, dass ein offener Dialog, Transparenz und gegenseitige Unterstützung entscheidend für den Erfolg und das Wachstum beider Seiten sind. Lieferanten, die Herausforderungen oder Bedenken im Hinblick auf die Erfüllung der Standards dieses Codes haben, sind eingeladen, frühzeitig das Gespräch mit uns zu suchen, um Lösungen zu erarbeiten.

Unsere Türen stehen immer offen für Rückfragen, Verbesserungsvorschläge oder Kooperationen, die darauf abzielen, die im Supplier Code of Conduct festgelegten Standards noch weiter zu optimieren. Unser gemeinsames Ziel ist es, durch partnerschaftliche Zusammenarbeit und klare ethische Prinzipien eine nachhaltige, erfolgreiche Zukunft zu gestalten.

1.4. Verbindlichkeit

Die Einhaltung des Supplier Code of Conduct ist ein verbindlicher Bestandteil jeder Geschäftsbeziehung mit der REMSA GmbH. Wir erwarten, dass unsere Lieferanten diese Anforderungen ernst nehmen und alle notwendigen Schritte unternehmen, um sicherzustellen, dass sie in allen Bereichen erfüllt werden. Verstöße gegen diesen Code können je nach Schwere der Abweichung zu Sanktionen bis hin zur Beendigung der Geschäftsbeziehung führen.

Lieferanten, die sich aktiv um die Einhaltung der im Supplier Code of Conduct festgelegten Standards bemühen, werden von der REMSA GmbH als vertrauenswürdige und langfristige Partner geschätzt. Wir freuen uns darauf, gemeinsam mit Ihnen eine erfolgreiche und nachhaltige Zukunft zu gestalten.

Kapitel 2: Einhaltung von Gesetzen und Vorschriften

Die REMSA GmbH erwartet von ihren Lieferanten, dass sie in allen Bereichen ihrer Geschäftstätigkeit die nationalen und internationalen Gesetze, Vorschriften und Regulierungen vollständig einhalten. Dies umfasst insbesondere Vorschriften im Bereich der Informationstechnologie, Datenschutzbestimmungen und rechtliche Rahmenbedingungen für die Entwicklung und Bereitstellung von Software. Jeder Verstoß gegen geltende Gesetze und Vorschriften kann nicht nur zu rechtlichen Konsequenzen, sondern auch zu einer Beendigung der Geschäftsbeziehung führen.

Die Einhaltung aller geltenden Gesetze und Vorschriften ist nicht nur eine rechtliche Notwendigkeit, sondern auch ein wesentlicher Bestandteil einer nachhaltigen und vertrauensvollen Partnerschaft. Die REMSA GmbH legt großen Wert darauf, dass alle Lieferanten verantwortungsbewusst handeln und die rechtlichen Rahmenbedingungen vollständig erfüllen.

2.1. IT-Sicherheitsumgebung

Lieferanten müssen sicherstellen, dass ihre Produkte und Dienstleistungen den geltenden Sicherheitsvorschriften entsprechen. Dies beinhaltet unter anderem:

- **Schutz vor Cyberbedrohungen**: Lieferanten müssen geeignete Maßnahmen treffen, um die Integrität, Vertraulichkeit und Verfügbarkeit ihrer IT-Systeme und Dienstleistungen zu gewährleisten.
- **Einhaltung nationaler und internationaler IT-Sicherheitsgesetze**: Dies umfasst etwa das deutsche IT-Sicherheitsgesetz sowie andere regionale und internationale Anforderungen, die auf den Schutz von IT-Systemen abzielen.

2.2. Datenschutz und DSGVO:

Lieferanten, die personenbezogene Daten verarbeiten, speichern oder übermitteln, müssen die EU-Datenschutz-Grundverordnung (DSGVO) sowie andere einschlägige Datenschutzgesetze einhalten. Dies bedeutet insbesondere:

- **Rechtmäßige Erhebung und Verarbeitung von Daten**: Alle personenbezogenen Daten müssen in Übereinstimmung mit den geltenden Datenschutzgesetzen erhoben und verarbeitet werden.
- **Datensicherheit und -schutz**: Lieferanten müssen angemessene technische und organisatorische Maßnahmen implementieren, um sicherzustellen, dass personenbezogene Daten geschützt und nicht unbefugt offengelegt oder manipuliert werden.
- **Datentransfers in Drittländer**: Wenn personenbezogene Daten in Länder außerhalb der EU übertragen werden, müssen Lieferanten sicherstellen, dass die Übermittlung den entsprechenden rechtlichen Anforderungen entspricht (z. B. Standardvertragsklauseln, Angemessenheitsentscheidungen).

2.3. Softwarelizenzierung und Urheberrecht

Die REMSA GmbH erwartet, dass Lieferanten alle geltenden Urheberrechtsgesetze und Bestimmungen im Zusammenhang mit Softwarelizenzen einhalten. Dies umfasst:

- **Lizenzkonformität**: Lieferanten müssen sicherstellen, dass alle von ihnen eingesetzten oder gelieferten Softwareprodukte ordnungsgemäß lizenziert sind und keine Urheberrechte verletzen.

- **Dokumentation und Nachweise**: Auf Anfrage muss der Lieferant der REMSA GmbH Lizenznachweise und -verträge vorlegen, um die Einhaltung der Lizenzanforderungen zu bestätigen.

2.4. Compliance im IT-Sektor

Lieferanten müssen sicherstellen, dass ihre Produkte, Dienstleistungen und Prozesse die branchenüblichen Compliance-Standards im IT-Sektor erfüllen. Dies kann beinhalten:

- **Cloud-Computing-Regulierungen**: Bei der Bereitstellung von Cloud-Diensten müssen Lieferanten sicherstellen, dass alle relevanten Gesetze und Standards zur Datenspeicherung und -verarbeitung eingehalten werden, insbesondere in Bezug auf Datensicherheit, Datenhoheit und Datenverfügbarkeit.
- **Offene Schnittstellen und Interoperabilität**: Lieferanten müssen sicherstellen, dass ihre IT-Produkte und -Dienstleistungen auf offenen und interoperablen Standards basieren, um die Integration in bestehende IT-Umgebungen zu erleichtern und Abhängigkeiten zu vermeiden.

2.5. Einhaltung von Wettbewerbs- und Handelsgesetzen

Die Lieferanten der REMSA GmbH müssen alle Vorschriften des fairen Wettbewerbs sowie nationale und internationale Handelsgesetze beachten. Dies bedeutet:

- **Verbot von Kartellabsprachen**: Lieferanten dürfen sich nicht an wettbewerbswidrigen Absprachen oder Praktiken beteiligen, die den freien Markt beeinträchtigen oder Kunden schädigen könnten.
- **Einhaltung von Exportkontrollgesetzen**: Insbesondere im IT-Sektor müssen Lieferanten sicherstellen, dass alle Exporte von Produkten oder Technologien den geltenden Exportkontrollgesetzen entsprechen.

2.6. Arbeitsschutz und Gesundheitsvorschriften

Lieferanten müssen sicherstellen, dass sie alle arbeitsrechtlichen Vorschriften in den Ländern, in denen sie tätig sind, einhalten. Dies umfasst insbesondere:

- **Gesundheits- und Sicherheitsstandards**: Sicherstellung, dass die Arbeitsplätze sicher und gesundheitsfreundlich gestaltet sind, insbesondere im Umgang mit Technologien und Maschinen.
- **Faire Arbeitszeiten und gerechte Bezahlung**: Alle Mitarbeiter müssen faire Arbeitsbedingungen haben, die den gesetzlichen Bestimmungen entsprechen.

2.7. Meldepflicht bei Gesetzesverstößen

Sollte ein Lieferant Kenntnis von einem potenziellen oder tatsächlichen Gesetzesverstoß in seinem Unternehmen oder in seiner Lieferkette erlangen, muss er dies unverzüglich der REMSA GmbH melden. Der Lieferant ist verpflichtet, entsprechende Maßnahmen zu ergreifen, um die Ursache des Verstoßes zu beheben und eine Wiederholung zu verhindern.

Kapitel 3: Arbeitsrechtliche und soziale Standards

Die REMSA GmbH verpflichtet sich zu fairen und ethischen Geschäftspraktiken und erwartet dasselbe von ihren Lieferanten. Die Einhaltung der grundlegenden Menschenrechte, fairer Arbeitsbedingungen und sozialer Verantwortung ist eine unerlässliche Voraussetzung für die Zusammenarbeit. Wir erwarten, dass unsere Lieferanten sicherstellen, dass diese Grundsätze in ihrem gesamten Betrieb und ihrer Lieferkette durchgesetzt werden.

3.1. Verbot von Kinderarbeit

Kinderarbeit ist in allen Formen strikt verboten. Lieferanten der REMSA GmbH dürfen keine Minderjährigen unter dem gesetzlich zulässigen Alter beschäftigen. Konkret bedeutet dies:

- Die Beschäftigung von Personen unter 15 Jahren (oder älter, wenn dies nach nationalem Recht erforderlich ist) ist untersagt, es sei denn, das nationale Recht erlaubt Arbeitsverhältnisse im Rahmen von Ausbildung oder Praktika.
- Der Lieferant muss sicherstellen, dass jugendliche Arbeitnehmer (über dem Mindestalter, aber unter 18 Jahren) nur Tätigkeiten ausführen, die keine Gefahr für ihre Gesundheit, Sicherheit oder Entwicklung darstellen. Dies umfasst insbesondere den Schutz vor physischen und psychischen Belastungen durch IT- oder technische Arbeiten.
- Programme für berufliche Ausbildungen und Praktika dürfen nur unter strikter Einhaltung der rechtlichen Vorschriften und zu fairen Konditionen angeboten werden.

3.2. Verbot von Zwangsarbeit

Jegliche Form von Zwangsarbeit, einschließlich unfreiwilliger Gefängnisarbeit, Sklaverei, Menschenhandel oder anderer Formen der Ausbeutung, ist verboten. Der Lieferant muss sicherstellen, dass:

- Alle Arbeitsverhältnisse freiwillig sind.
- Arbeitnehmer das Recht haben, ihre Beschäftigung mit einer angemessenen Kündigungsfrist zu beenden, ohne dass ihnen dadurch Strafmaßnahmen drohen.
- Keine persönlichen Dokumente wie Reisepässe, Arbeitsgenehmigungen oder andere persönliche Gegenstände einbehalten werden, um Arbeitnehmer an der freien Wahl ihres Arbeitsplatzes zu hindern.

3.3. Diskriminierungsverbot

Diskriminierung jeglicher Art in Bezug auf Geschlecht, Alter, Religion, ethnische Herkunft, sexuelle Orientierung, Behinderung oder andere persönliche Merkmale ist streng verboten. Lieferanten müssen sicherstellen, dass:

- Rekrutierung, Vergütung, Schulungen, Beförderungen, Kündigungen und andere arbeitsbezogene Entscheidungen allein auf der Basis von Qualifikationen, Leistung, Fähigkeiten und Erfahrung erfolgen.
- Ein Arbeitsumfeld geschaffen wird, das frei von Belästigung, Diskriminierung und Gewalt ist.
- Gleiche Entlohnung für gleiche Arbeit unabhängig von Geschlecht oder anderen persönlichen Merkmalen gewährleistet wird.

- Sensibilisierungstrainings oder Maßnahmen zur Förderung der Vielfalt und Inklusion in die Unternehmenskultur integriert werden.

3.4. Faire Arbeitsbedingungen

Die REMSA GmbH erwartet von ihren Lieferanten, dass sie den Mitarbeitern faire Arbeitsbedingungen bieten, die den gesetzlichen und ethischen Standards entsprechen:

- **Arbeitszeiten**: Die gesetzlichen Arbeitszeiten der jeweiligen Länder müssen eingehalten werden. Eine angemessene Freizeit, Ruhezeiten und Pausen müssen gewährleistet sein. In der IT-Branche, in der Überstunden oft vorkommen können, muss sichergestellt sein, dass alle Überstunden freiwillig sind und fair entlohnt werden.
- **Vergütung**: Löhne und Gehälter müssen mindestens dem gesetzlichen Mindestlohn entsprechen oder über diesem liegen, falls anwendbar. Alle Arbeitnehmer haben das Recht auf pünktliche und transparente Zahlungen ohne unrechtmäßige Abzüge. Darüber hinaus sollen leistungsbezogene Prämien oder Anreize, falls angeboten, fair und nachvollziehbar gestaltet sein.
- **Vertragliche Klarheit**: Alle Arbeitnehmer müssen rechtzeitig schriftliche Arbeitsverträge erhalten, die klare Informationen über ihre Aufgaben, Vergütung, Arbeitszeiten und Bedingungen enthalten.

3.5. Vereinigungsfreiheit und Recht auf Kollektivverhandlungen

Lieferanten müssen das Recht ihrer Mitarbeiter auf Vereinigungsfreiheit respektieren und sicherstellen, dass sie sich ohne Angst vor Repressalien gewerkschaftlich organisieren können. Dies bedeutet konkret:

- Das Recht der Mitarbeiter auf Gründung oder Beitritt zu Gewerkschaften oder ähnlichen Organisationen darf nicht behindert oder eingeschränkt werden.
- Kollektivverhandlungen zwischen Arbeitnehmern und Arbeitgebern müssen nach den gesetzlichen Vorgaben unterstützt werden, um Arbeitsbedingungen und -standards auszuhandeln.
- Wo Gewerkschaften gesetzlich nicht zugelassen oder traditionell nicht vorhanden sind, müssen alternative Möglichkeiten der Mitarbeitervertretung unterstützt werden.

3.6. Gesundheit und Sicherheit am Arbeitsplatz

Die REMSA GmbH erwartet von ihren Lieferanten, dass sie sichere und gesunde Arbeitsbedingungen schaffen, um die physische und psychische Gesundheit der Mitarbeiter zu gewährleisten:

- **Sicherheitsvorkehrungen**: Lieferanten müssen in ihren Arbeitsbereichen angemessene Sicherheitsvorkehrungen treffen, insbesondere im Bereich der IT, wo der ergonomische Arbeitsplatz, Bildschirmarbeit und sichere Arbeitsumgebungen von zentraler Bedeutung sind.
- **Gefährdungsbeurteilungen und Notfallpläne**: Regelmäßige Gefährdungsbeurteilungen müssen durchgeführt und geeignete Notfallpläne entwickelt werden, um das Risiko von Unfällen oder gesundheitlichen Gefahren zu minimieren.
- **Ergonomie und Gesundheit**: Insbesondere in der IT-Branche, in der Bildschirmarbeit häufig ist, muss darauf geachtet werden, dass die Arbeitsplätze ergonomisch gestaltet sind, um Langzeitschäden vorzubeugen. Regelmäßige Pausen und Bewegungsmöglichkeiten sind zu fördern.
- **Schulung und Sensibilisierung**: Mitarbeiter müssen regelmäßig zu Themen wie Arbeitssicherheit, Gesundheitsschutz und Erste Hilfe geschult werden.

3.7. Schutz von Whistleblowern

Lieferanten müssen sicherstellen, dass Mitarbeiter, die Verstöße gegen ethische Standards oder rechtliche Vorgaben melden, vor Repressalien geschützt werden. Der Schutz von Whistleblowern muss durch geeignete Mechanismen gewährleistet werden, um ihre Anonymität zu wahren und sie vor möglichen negativen Konsequenzen zu schützen.

3.8. Verbot von Belästigung, Gewalt und Mobbing

Lieferanten müssen ein Arbeitsumfeld schaffen, das frei von jeglicher Form der Belästigung, Mobbing und Gewalt ist. Dazu gehören insbesondere:

- Präventivmaßnahmen zur Vermeidung von psychischen und physischen Übergriffen, Belästigung oder unethischem Verhalten am Arbeitsplatz.
- Ein effektives Beschwerdesystem, das es den Mitarbeitern ermöglicht, Probleme oder Missstände vertraulich und ohne Angst vor Vergeltungsmaßnahmen zu melden.

Kapitel 4: Umweltschutz und Nachhaltigkeit

Die REMSA GmbH legt großen Wert auf nachhaltiges und umweltfreundliches Wirtschaften und erwartet dasselbe von ihren Lieferanten. In der IT-Branche spielen Umweltaspekte eine wichtige Rolle, insbesondere durch den Energieverbrauch von IT-Systemen, die Herstellung von Hardware und die Entsorgung von Elektronikabfällen. Lieferanten müssen nachhaltige Praktiken anwenden, um negative Umweltauswirkungen zu minimieren und die natürlichen Ressourcen zu schonen. Dies trägt nicht nur zum Umweltschutz bei, sondern unterstützt auch langfristig die Stabilität der Geschäftsbeziehungen.

4.1. Einhaltung von Umweltgesetzen und -vorschriften

Lieferanten müssen alle relevanten nationalen und internationalen Umweltgesetze und -vorschriften einhalten. Dies umfasst insbesondere:

- **Gesetze zur Reduzierung von Treibhausgasemissionen**: Alle Vorschriften zur Reduzierung von CO2-Emissionen und anderen Treibhausgasen müssen eingehalten werden.
- **Vorschriften zur Abfallentsorgung**: Lieferanten müssen sicherstellen, dass alle entstehenden Abfälle ordnungsgemäß entsorgt oder recycelt werden, insbesondere bei der Herstellung und Entsorgung von IT-Hardware.
- **Compliance im Umgang mit gefährlichen Stoffen**: Es dürfen keine umweltschädlichen Materialien verwendet werden, die gegen internationale Gesetze wie RoHS (Restriction of Hazardous Substances) oder REACH (Registration, Evaluation, Authorisation and Restriction of Chemicals) verstoßen.

4.2. Ressourcenschonende Produktion und Lieferketten

Lieferanten der REMSA GmbH müssen Maßnahmen ergreifen, um den Einsatz von Ressourcen effizient zu gestalten und Verschwendung zu minimieren. Dazu gehören:

- **Reduzierung des Energieverbrauchs**: IT-Produkte, die hergestellt werden, sollten energieeffizient sein und die neuesten Standards in Bezug auf Stromverbrauch und Energieeffizienz einhalten (z. B. ENERGY STAR-zertifizierte Produkte). Lieferanten sollten Maßnahmen ergreifen, um ihre eigenen Produktionsprozesse energieeffizient zu gestalten und den Einsatz von erneuerbaren Energien zu fördern.
- **Ressourceneffizienz in der Produktion**: Lieferanten müssen sicherstellen, dass der Ressourcenverbrauch bei der Herstellung von IT-Hardware und Software minimal ist. Dies umfasst insbesondere die Reduzierung von Wasser-, Material- und Energieverbrauch.
- **Nachhaltige Beschaffung**: Lieferanten sollten bevorzugt Materialien und Komponenten aus nachhaltigen Quellen beziehen und sicherstellen, dass in ihrer Lieferkette keine Materialien aus konfliktbelasteten Regionen verwendet werden (z. B. keine Konfliktmineralien).

4.3. E-Waste-Management und Recycling

Elektronische Abfälle (E-Waste) stellen eine große Herausforderung in der IT-Branche dar. Lieferanten müssen sicherstellen, dass alle IT-Produkte, die sie liefern oder herstellen, umweltgerecht recycelt oder entsorgt werden:

- **Vermeidung von E-Waste**: Lieferanten sollten den Lebenszyklus von IT-Hardware maximieren, indem sie Produkte herstellen, die langlebig, reparierbar und aufrüstbar sind, anstatt auf Einwegprodukte zu setzen.
- **Recycling und Wiederverwertung**: Lieferanten müssen Recycling- und Wiederverwertungsprogramme für ihre Produkte und Komponenten unterstützen. Dies umfasst die Rücknahme von Altgeräten, die sichere Entsorgung von Elektronikschrott und die Wiederverwendung von Rohstoffen.
- **Verantwortungsvolle Entsorgung von gefährlichen Abfällen**: Elektronische Produkte können gefährliche Stoffe wie Blei, Quecksilber und andere toxische Materialien enthalten. Lieferanten müssen sicherstellen, dass diese Stoffe gemäß den Umweltstandards sicher entsorgt werden.

4.4. Minimierung von Treibhausgasemissionen zum Klimaschutz

IT-Unternehmen und Hardwarehersteller sowie Händler tragen erheblich zum globalen Energieverbrauch bei, insbesondere durch den Betrieb von Rechenzentren und Cloud-Diensten. Lieferanten müssen Maßnahmen ergreifen, um ihre Emissionen zu reduzieren und den Klimaschutz zu unterstützen:

- **Reduzierung des CO2-Fußabdrucks**: Lieferanten müssen den Energieverbrauch und die Emissionen ihrer Rechenzentren, Produktionsstätten und Logistikprozesse optimieren, um den CO2-Ausstoß zu minimieren. Dazu sollten sie moderne, energieeffiziente Technologien einsetzen.
- **Förderung von erneuerbaren Energien**: Lieferanten sollen, wo immer möglich, erneuerbare Energien wie Solar- oder Windkraft nutzen, um den Stromverbrauch ihrer Systeme und Prozesse zu decken. Rechenzentren sollten auf eine saubere Energiequelle umgestellt werden.
- **Nachhaltige Logistik**: Lieferanten sollten ihre Transportprozesse optimieren, um Emissionen zu reduzieren. Dies kann durch eine verbesserte Routenplanung, den Einsatz von emissionsarmen Transportmitteln oder die Minimierung von Verpackungsmaterialien erreicht werden.

4.5. Förderung von umweltfreundlichen Technologien

Lieferanten der REMSA GmbH sollten innovative, umweltfreundliche Technologien fördern, um den ökologischen Fußabdruck der IT-Industrie zu reduzieren:

- **Cloud Computing und Virtualisierung**: Cloud-basierte Lösungen und Virtualisierungstechnologien können den physischen Hardwarebedarf reduzieren und den Energieverbrauch erheblich senken. Lieferanten sollten nachhaltige Cloud-Dienste bereitstellen, die energieeffizient betrieben werden.
- **Künstliche Intelligenz für Umweltschutz**: Der Einsatz von Künstlicher Intelligenz (KI) zur Optimierung von Energieverbrauch und Ressourcennutzung sollte unterstützt werden. Dies kann zur Verbesserung der Effizienz von Produktions- und Geschäftsprozessen beitragen und gleichzeitig die Umweltbelastung verringern.
- **Förderung nachhaltiger Softwareentwicklung**: Lieferanten sollten umweltfreundliche Softwarelösungen entwickeln, die energieeffizient arbeiten und den Hardwarebedarf minimieren. Dazu gehören auch Bemühungen, die Langlebigkeit und Aufrüstbarkeit von IT-Lösungen zu gewährleisten.

4.6. Transparenz in der Umweltberichterstattung

Die REMSA GmbH erwartet von ihren Lieferanten eine transparente Berichterstattung über ihre Umweltpraktiken. Lieferanten müssen regelmäßig über ihre Umweltziele, ihre Fortschritte bei der Emissionsreduktion und ihre Recyclingprogramme berichten. Dies umfasst:

- **Umweltmanagementsysteme**: Lieferanten sollten ein Umweltmanagementsystem einführen und pflegen, um ihre Umweltpraktiken zu überwachen und kontinuierlich zu verbessern. Idealerweise sind Lieferanten nach ISO 14001 oder ähnlichen Standards zertifiziert.
- **Umweltkennzahlen und Berichte**: Lieferanten müssen ihre Umweltauswirkungen messen und regelmäßig Umweltberichte vorlegen, die ihre Fortschritte bei der Reduzierung von Emissionen, Energieverbrauch und Abfall dokumentieren.
- **Ziele zur kontinuierlichen Verbesserung**: Lieferanten müssen sich dazu verpflichten, ihre Umweltpraktiken kontinuierlich zu verbessern und klare Ziele zur Reduzierung ihres ökologischen Fußabdrucks zu setzen.

Kapitel 5: Menschenrechte und IT-Compliance

Die REMSA GmbH verpflichtet sich, die grundlegenden Menschenrechte in allen Aspekten ihres Geschäfts zu wahren, und erwartet dasselbe von ihren Lieferanten. Als IT-Unternehmen sind wir uns bewusst, dass technologische Entwicklungen erhebliche Auswirkungen auf Menschen und Gesellschaft haben können. Daher erwarten wir von unseren Lieferanten, dass sie die Menschenrechte achten und IT-Compliance sicherstellen, um Missbrauch zu verhindern und den positiven Einfluss der Technologie zu fördern.

5.1. Achtung der Menschenrechte

Lieferanten müssen die Menschenrechte respektieren und aktiv dazu beitragen, Verletzungen dieser Rechte zu verhindern. Dies schließt alle Aspekte der Beschäftigung und der Geschäftstätigkeit ein:

- **Verbot von Menschenrechtsverletzungen**: Lieferanten dürfen sich weder direkt noch indirekt an Menschenrechtsverletzungen beteiligen. Dies schließt Zwangsarbeit, Ausbeutung, Menschenhandel und jede Form der modernen Sklaverei ein.
- **Verantwortungsvolle Geschäftspraktiken**: Lieferanten müssen sicherstellen, dass ihre Geschäftspraktiken ethisch und verantwortungsbewusst gestaltet sind. Insbesondere in der IT-Branche ist es wichtig, dass technologische Entwicklungen weder Menschen noch gesellschaftliche Strukturen negativ beeinflussen.
- **Schutz der Arbeitnehmerrechte**: Lieferanten müssen dafür sorgen, dass alle Arbeitnehmer fair und mit Respekt behandelt werden, unabhängig von ihrer Herkunft, ihrem Geschlecht, ihrer sexuellen Orientierung oder anderen persönlichen Merkmalen. Diskriminierung, Mobbing und andere Formen der Ungleichbehandlung sind verboten.
- **Konsultation und Einbindung der Mitarbeiter**: Lieferanten müssen den Arbeitnehmern die Möglichkeit geben, an Entscheidungsprozessen teilzunehmen, die ihre Arbeitsbedingungen oder ihre Menschenrechte betreffen.

5.2. IT-Compliance und Verantwortung

In der IT-Branche spielen Datenschutz, IT-Sicherheit und die ethische Nutzung von Technologien eine zentrale Rolle. Lieferanten der REMSA GmbH müssen sicherstellen, dass ihre IT-Systeme und -Dienstleistungen die höchsten Standards der Compliance und der technologischen Verantwortung erfüllen:

- **Einhaltung der Datenschutzvorschriften**: Lieferanten müssen die geltenden Datenschutzgesetze einhalten, insbesondere die europäische Datenschutz-Grundverordnung (DSGVO) sowie weitere nationale und internationale Regelungen. Personenbezogene Daten müssen sicher und verantwortungsvoll behandelt werden.
- **Vermeidung von Technologiemissbrauch**: Lieferanten dürfen keine Technologien entwickeln oder bereitstellen, die zu Menschenrechtsverletzungen führen könnten. Dazu gehören insbesondere Überwachungstechnologien, die zur unrechtmäßigen Kontrolle von Personen oder zur Verletzung der Privatsphäre eingesetzt werden könnten.
- **Verantwortungsvoller Umgang mit KI und Automatisierung**: Lieferanten, die Künstliche Intelligenz (KI), Automatisierung und maschinelles Lernen einsetzen, müssen sicherstellen, dass diese Technologien ethisch genutzt werden. Der Einsatz von KI darf nicht zu Diskriminierung, Ausgrenzung oder Missbrauch führen.

- **Schutz von Daten und IT-Systemen**: IT-Lieferanten müssen angemessene Sicherheitsvorkehrungen treffen, um ihre Systeme und die der Kunden vor Cyberangriffen, Datenlecks oder unerlaubtem Zugriff zu schützen. Dies umfasst die Einhaltung internationaler Sicherheitsstandards, regelmäßige Sicherheitsüberprüfungen und die sofortige Behebung von Schwachstellen.

5.3. Vermeidung von Missbrauch durch Technologien

Lieferanten der REMSA GmbH müssen sicherstellen, dass ihre Technologien und Dienstleistungen keine negativen sozialen Auswirkungen haben:

- **Technologien, die Menschenrechte schützen**: Lieferanten sollen Technologien fördern und entwickeln, die den Schutz der Menschenrechte unterstützen, wie z. B. Verschlüsselungstechnologien, die die Privatsphäre wahren, oder Programme, die den Zugang zu Bildung und Information fördern.
- **Verantwortungsvolle Nutzung von Daten**: Lieferanten müssen gewährleisten, dass Daten, die sie sammeln oder verarbeiten, verantwortungsvoll genutzt werden. Dazu gehört die Vermeidung der Erhebung unnötiger Daten, die Minimierung der Datenspeicherung und die Sicherstellung, dass keine sensiblen Daten missbraucht oder für diskriminierende Zwecke verwendet werden.
- **Kein Einsatz von Technologien zur Überwachung und Kontrolle**: Technologien, die das Potenzial haben, zur unrechtmäßigen Überwachung oder Kontrolle von Personen eingesetzt zu werden, dürfen von Lieferanten nicht entwickelt, produziert oder bereitgestellt werden.

5.4. Verantwortung in der Lieferkette

Lieferanten müssen sicherstellen, dass auch ihre eigenen Zulieferer und Geschäftspartner die Menschenrechte respektieren und die Standards der IT-Compliance einhalten. Dies umfasst:

- **Due-Diligence-Verfahren**: Lieferanten müssen regelmäßig überprüfen, ob ihre Zulieferer den Menschenrechten und ethischen Standards gerecht werden. Dies kann durch Audits, Zertifizierungen oder andere Überprüfungen geschehen.
- **Weitergabe von Compliance-Anforderungen**: Lieferanten müssen sicherstellen, dass auch in der eigenen Lieferkette die Anforderungen an Datenschutz, IT-Sicherheit und ethische Geschäftspraktiken umgesetzt werden.

5.5. Whistleblower-Schutz

Lieferanten müssen Mechanismen einrichten, die es den Mitarbeitern ermöglichen, Menschenrechtsverletzungen, Datenschutzverstöße oder andere ethische Bedenken anonym und ohne Angst vor Repressalien zu melden:

- **Vertrauliche Meldung**: Es muss eine sichere und vertrauliche Möglichkeit für Mitarbeiter geben, Verstöße zu melden. Diese Meldungen müssen ernst genommen und zügig geprüft werden.
- **Schutz vor Vergeltungsmaßnahmen**: Mitarbeiter, die Verstöße gegen Menschenrechte oder IT-Compliance-Anforderungen melden, dürfen keine Nachteile oder Vergeltungsmaßnahmen erfahren. Der Schutz von Whistleblowern ist ein zentrales Element ethischer Geschäftspraktiken.

5.6. Nachhaltige ethische Geschäftspraktiken

Lieferanten müssen nicht nur ethische Geschäftspraktiken einhalten, sondern auch sicherstellen, dass ihre Technologien und Geschäftspraktiken zur Förderung einer nachhaltigen und gerechten Gesellschaft beitragen:

- **Ethische Innovation**: Neue technologische Entwicklungen müssen darauf abzielen, positive soziale Auswirkungen zu haben. Dies bedeutet, dass ethische Überlegungen in den Innovationsprozess integriert werden müssen.
- **Förderung der sozialen Verantwortung**: Lieferanten müssen Programme entwickeln oder unterstützen, die zur Verbesserung der Gemeinschaft beitragen, wie z. B. Bildungsprogramme, Initiativen zur digitalen Inklusion oder Projekte, die den Zugang zu Technologie in benachteiligten Regionen verbessern.

Kapitel 6: IT-Sicherheit und Datenschutz

In der modernen Geschäftswelt ist IT-Sicherheit von entscheidender Bedeutung, insbesondere für Unternehmen im IT-Sektor wie die REMSA GmbH. Unsere Lieferanten spielen eine wesentliche Rolle beim Schutz sensibler Informationen, Systeme und Daten. Wir erwarten von unseren Lieferanten, dass sie die höchsten Standards der IT-Sicherheit und des Datenschutzes einhalten und sich an alle geltenden gesetzlichen Bestimmungen halten. Der Schutz von Daten und der verantwortungsbewusste Umgang mit Informationen sind wesentliche Voraussetzungen für eine vertrauensvolle Zusammenarbeit.

6.1. Einhaltung der Datenschutzgesetze

Lieferanten der REMSA GmbH müssen alle geltenden Datenschutzgesetze und -vorschriften einhalten, insbesondere:

- **EU-Datenschutz-Grundverordnung (DSGVO)**: Lieferanten, die personenbezogene Daten von EU-Bürgern verarbeiten, müssen sicherstellen, dass sie die Anforderungen der DSGVO vollständig erfüllen. Dies umfasst die rechtskonforme Erhebung, Verarbeitung, Speicherung und Übermittlung von personenbezogenen Daten.
- **Nationale Datenschutzgesetze**: Lieferanten müssen zusätzlich zu internationalen Standards auch die spezifischen Datenschutzgesetze der Länder einhalten, in denen sie tätig sind.

Zu den wichtigen Anforderungen gehören:

- **Rechtmäßige Datenerhebung**: Personenbezogene Daten dürfen nur erhoben werden, wenn eine rechtmäßige Grundlage dafür besteht, wie z. B. Einwilligung, Vertragserfüllung oder ein berechtigtes Interesse.
- **Datenminimierung**: Nur die Daten, die für den spezifischen Zweck erforderlich sind, dürfen erhoben und verarbeitet werden.
- **Datenaufbewahrung und -löschung**: Personenbezogene Daten dürfen nur so lange aufbewahrt werden, wie es der Zweck der Datenverarbeitung erfordert. Nach Erfüllung des Zwecks müssen Daten sicher gelöscht werden.

6.2. Technische und organisatorische Maßnahmen (TOMs)

Lieferanten müssen angemessene technische und organisatorische Maßnahmen (TOMs) ergreifen, um die Sicherheit und Vertraulichkeit von Informationen zu gewährleisten. Diese Maßnahmen dienen dem Schutz vor unberechtigtem Zugriff, Datenverlust, Cyberangriffen und anderen Bedrohungen. Zu den TOMs gehören:

- **Verschlüsselung von Daten**: Sensible Daten müssen während der Übertragung (z. B. per E-Mail) und im Ruhezustand (z. B. auf Servern) verschlüsselt werden, um sie vor unberechtigtem Zugriff zu schützen.
- **Zugriffskontrollen**: Lieferanten müssen sicherstellen, dass nur autorisierte Personen Zugriff auf sensible Informationen haben. Dies umfasst die Einführung von Multi-Faktor-Authentifizierung, Rollen-basierter Zugriffskontrolle und der regelmäßigen Überprüfung von Berechtigungen.
- **Sicherheitsupdates und Patches**: Lieferanten müssen ihre Systeme regelmäßig aktualisieren und Sicherheitsupdates einspielen, um bekannte Schwachstellen zu schließen und das Risiko von Cyberangriffen zu minimieren.

- **Firewalls und Virenschutz**: Alle IT-Systeme müssen durch geeignete Sicherheitslösungen wie Firewalls, Intrusion Detection Systems (IDS) und Antivirenprogramme geschützt werden, um Bedrohungen frühzeitig zu erkennen und abzuwehren.

6.3. Schutz von Kundendaten

Die REMSA GmbH legt großen Wert auf den Schutz von Kundendaten. Lieferanten, die Zugang zu vertraulichen Kundendaten haben oder diese im Rahmen ihrer Dienstleistung verarbeiten, müssen sicherstellen, dass diese Daten mit größter Sorgfalt behandelt werden:

- **Vertraulichkeitserklärung**: Lieferanten müssen eine schriftliche Vertraulichkeitserklärung unterzeichnen, die sicherstellt, dass alle Kundendaten vertraulich behandelt und nicht an Dritte weitergegeben werden.
- **Datensicherheitsrichtlinien**: Lieferanten müssen interne Richtlinien zur Datensicherheit haben, die den Umgang mit sensiblen Daten regeln und sicherstellen, dass alle Mitarbeiter mit diesen Richtlinien vertraut sind.
- **Datenübertragung**: Jegliche Übertragung von Kundendaten, insbesondere personenbezogene Daten, muss sicher verschlüsselt erfolgen. Dies gilt für den Austausch per E-Mail, Dateifreigabe oder andere digitale Kommunikationsmittel.

6.4. Verantwortung für Cybersicherheit

Lieferanten müssen sicherstellen, dass ihre IT-Systeme robust gegen Cyberangriffe sind. Dazu gehört die proaktive Überwachung und Sicherung von Netzwerken, Systemen und Daten:

- **Erkennung und Reaktion auf Sicherheitsvorfälle**: Lieferanten müssen über Mechanismen verfügen, um Sicherheitsvorfälle wie Cyberangriffe oder Datenverluste schnell zu erkennen, darauf zu reagieren und entsprechende Maßnahmen zu ergreifen.
- **Incident-Management-Prozesse**: Im Falle eines Sicherheitsvorfalls müssen Lieferanten ein etabliertes Verfahren haben, um die Ursache des Vorfalls zu ermitteln, die Auswirkungen zu minimieren und die REMSA GmbH unverzüglich zu informieren.
- **Notfall- und Wiederherstellungspläne**: Lieferanten müssen über Notfallpläne verfügen, um die Wiederherstellung kritischer IT-Systeme und Daten zu gewährleisten, falls es zu einem Ausfall oder einer Störung kommt.

6.5. Datenverarbeitung durch Dritte

Lieferanten, die Unterauftragnehmer oder Dritte mit der Verarbeitung von Daten beauftragen, müssen sicherstellen, dass diese ebenfalls die Anforderungen der IT-Sicherheit und des Datenschutzes erfüllen. Zu den wichtigsten Pflichten gehören:

- **Vertragliche Regelungen**: Lieferanten müssen sicherstellen, dass Dritte, die Daten im Auftrag verarbeiten, durch vertragliche Vereinbarungen an die gleichen Datenschutz- und Sicherheitsstandards gebunden sind.
- **Sorgfältige Auswahl von Dienstleistern**: Bevor ein Unterauftragnehmer beauftragt wird, müssen Lieferanten sicherstellen, dass diese angemessenen Sicherheitsmaßnahmen und Datenschutzrichtlinien implementiert hat.

- **Regelmäßige Audits und Überprüfungen**: Lieferanten sollten regelmäßige Audits bei Unterauftragnehmern durchführen, um sicherzustellen, dass die Sicherheitsstandards eingehalten werden.

6.6. Schulung und Sensibilisierung

Lieferanten müssen sicherstellen, dass alle Mitarbeiter, die Zugang zu sensiblen Daten oder IT-Systemen haben, regelmäßig zu IT-Sicherheit und Datenschutz geschult werden. Diese Schulungen sollten Folgendes umfassen:

- **Sensibilisierung für Sicherheitsbedrohungen**: Mitarbeiter müssen auf potenzielle Bedrohungen wie Phishing, Social Engineering und andere Angriffsarten aufmerksam gemacht werden.
- **Verantwortungsvoller Umgang mit Daten**: Mitarbeiter müssen geschult werden, wie sie mit sensiblen Informationen umgehen, sichere Passwörter verwenden und sicherstellen, dass ihre Systeme ordnungsgemäß geschützt sind.
- **Notfallverfahren**: Mitarbeiter müssen wissen, wie sie im Falle eines Sicherheitsvorfalls oder eines Datenschutzverstoßes zu handeln haben, um den Schaden zu begrenzen und den Vorfall zu melden.

6.7. Meldung von Sicherheitsvorfällen

Sollte es zu einem Verstoß gegen die IT-Sicherheit oder den Datenschutz kommen, müssen Lieferanten unverzüglich die REMSA GmbH informieren und geeignete Maßnahmen ergreifen, um den Vorfall zu beheben. Dazu gehören:

- **Sofortige Meldung**: Sicherheitsvorfälle müssen innerhalb eines festgelegten Zeitrahmens gemeldet werden (z. B. innerhalb von 24 Stunden nach Feststellung des Vorfalls).
- **Schadensbegrenzung**: Lieferanten müssen Maßnahmen ergreifen, um den Schaden zu begrenzen und betroffene Daten zu schützen.
- **Untersuchung und Berichterstattung**: Lieferanten müssen den Vorfall untersuchen, die Ursachen identifizieren und einen umfassenden Bericht über die Maßnahmen zur Behebung des Problems vorlegen.

Kapitel 7: Korruptionsbekämpfung und ethische Geschäftspraktiken

Die REMSA GmbH setzt sich für höchste ethische Standards in allen Geschäftsbeziehungen ein und erwartet dasselbe von ihren Lieferanten. Korruption, Bestechung und unethische Geschäftspraktiken untergraben das Vertrauen und die Integrität der Zusammenarbeit. Um langfristige, transparente und faire Partnerschaften zu fördern, verpflichtet sich die REMSA GmbH, nur mit Lieferanten zusammenzuarbeiten, die sich klar gegen Korruption stellen und ethisch korrekt handeln.

7.1. Verbot von Korruption und Bestechung

Lieferanten dürfen sich weder direkt noch indirekt an Korruption oder Bestechung beteiligen. Sie müssen sicherstellen, dass alle Geschäftspraktiken transparent und im Einklang mit den geltenden Gesetzen stehen. Dies umfasst insbesondere:

- **Verbot von Bestechung**: Lieferanten dürfen keine Bestechungsgelder anbieten, fordern oder annehmen, um sich einen geschäftlichen Vorteil zu verschaffen. Dies gilt sowohl für direkte Zahlungen als auch für indirekte Vorteile wie Geschenke, Vergünstigungen oder Dienstleistungen.
- **Umgang mit Amtsträgern und Behörden**: Jegliche Form von Bestechung oder unzulässiger Beeinflussung von Regierungsbeamten, Amtsträgern oder anderen öffentlichen Entscheidungsträgern ist strengstens verboten.
- **Keine unrechtmäßigen Zuwendungen**: Geschenke, Einladungen, Bewirtungen oder andere Vorteile dürfen nicht mit der Absicht angeboten werden, den Empfänger zu einer unlauteren Handlung zu bewegen oder eine unangemessene Beeinflussung auszuüben. Solche Zuwendungen sind nur in einem Rahmen erlaubt, der üblich, transparent und in Übereinstimmung mit den geltenden Vorschriften ist.

7.2. Vermeidung von Interessenkonflikten

Lieferanten müssen sicherstellen, dass potenzielle Interessenkonflikte, die ihre Geschäftstätigkeit beeinflussen könnten, vermieden werden. Dazu gehören:

- **Offenlegung von Beziehungen**: Lieferanten müssen jede Situation melden, in der persönliche oder geschäftliche Beziehungen zu einem Mitarbeiter der REMSA GmbH oder dessen Familie bestehen, die potenziell zu einem Interessenkonflikt führen könnten.
- **Geschäftliche Entscheidungen**: Geschäftliche Entscheidungen dürfen nicht durch persönliche Interessen oder Beziehungen beeinflusst werden. Alle Entscheidungen müssen zum Wohl des Unternehmens und auf der Grundlage objektiver Kriterien getroffen werden.

7.3. Geschenke und Einladungen

Der Umgang mit Geschenken und Einladungen muss mit größter Vorsicht erfolgen, um den Anschein von Bestechung oder unzulässiger Beeinflussung zu vermeiden:

- **Angemessene Geschenke**: Geschenke und Einladungen dürfen nur in einem angemessenen Rahmen und im Einklang mit den geschäftlichen Gepflogenheiten gemacht werden. Sie dürfen nicht den Eindruck erwecken, dass sie eine Gegenleistung für geschäftliche Vorteile sind.

- **Grenzen für Zuwendungen**: Lieferanten müssen sicherstellen, dass alle Zuwendungen (Geschenke, Einladungen, Bewirtungen) transparent und in Übereinstimmung mit den internen Richtlinien und gesetzlichen Vorgaben erfolgen. Geldgeschenke sind grundsätzlich untersagt.
- **Klare Richtlinien**: Lieferanten sollten über interne Richtlinien verfügen, die den Umgang mit Geschenken und Einladungen klar regeln und sicherstellen, dass diese nicht zur Korruption führen können.

7.4. Faire Wettbewerbspraktiken

Lieferanten der REMSA GmbH müssen sicherstellen, dass sie den Wettbewerb auf faire Weise fördern und keine wettbewerbswidrigen Praktiken anwenden. Dies umfasst:

- **Verbot von Kartellabsprachen**: Lieferanten dürfen sich nicht an Absprachen mit Wettbewerbern beteiligen, die den Markt oder den Wettbewerb einschränken. Preisabsprachen, Marktaufteilungen und andere kartellrechtswidrige Absprachen sind verboten.
- **Einhaltung von Wettbewerbsrecht**: Lieferanten müssen alle geltenden Gesetze und Vorschriften des Wettbewerbsrechts einhalten und sicherstellen, dass sie keine Marktmanipulationen oder unfaire Geschäftspraktiken anwenden.

7.5. Bekämpfung von Geldwäsche

Lieferanten müssen Maßnahmen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung ergreifen. Dies bedeutet, dass:

- **Sorgfaltspflichten**: Lieferanten müssen bei Geschäftsbeziehungen sorgfältig vorgehen und sicherstellen, dass ihre Partner und Unterauftragnehmer keine Geldwäscheaktivitäten durchführen.
- **Verdächtige Aktivitäten melden**: Jeder Verdacht auf Geldwäsche oder Terrorismusfinanzierung muss unverzüglich gemeldet und durch geeignete Maßnahmen verhindert werden.

7.6. Whistleblowing und Schutz von Hinweisgebern

Die REMSA GmbH unterstützt die Meldung von Verstößen gegen ethische Standards oder rechtliche Vorgaben durch Whistleblower. Lieferanten müssen sicherstellen, dass:

- **Sichere Meldekanäle**: Lieferanten müssen sichere und anonyme Meldekanäle bereitstellen, über die Mitarbeiter und Geschäftspartner Verstöße gegen ethische Standards, Korruption oder andere Unregelmäßigkeiten melden können.
- **Schutz von Whistleblowern**: Hinweisgeber müssen vor jeglicher Form von Repressalien geschützt werden. Es dürfen keine negativen Konsequenzen für Mitarbeiter entstehen, die in gutem Glauben Verstöße melden.
- **Untersuchung und Maßnahmen**: Jeder gemeldete Verstoß muss ernsthaft untersucht und angemessene Maßnahmen ergriffen werden, um Missstände zu beheben.

Kapitel 8: Transparenz und Zusammenarbeit

Die REMSA GmbH strebt nach langfristigen, offenen und vertrauensvollen Partnerschaften mit ihren Lieferanten. Transparenz in den Geschäftspraktiken und eine enge Zusammenarbeit sind wesentliche Voraussetzungen, um sicherzustellen, dass alle Standards und Erwartungen erfüllt werden. Um die Qualität und Integrität unserer Zusammenarbeit zu gewährleisten, ist es entscheidend, dass Lieferanten ihre Geschäftsprozesse offenlegen, auf Audits vorbereitet sind und bereitwillig kooperieren.

8.1. Offene und transparente Geschäftspraktiken

Die REMSA GmbH erwartet von ihren Lieferanten, dass sie alle relevanten Informationen zu ihren Geschäftspraktiken, Produktionsprozessen und Lieferketten transparent darlegen:

- **Offenlegung von Informationen**: Lieferanten müssen bereit sein, der REMSA GmbH alle relevanten Informationen über ihre Geschäftspraktiken zur Verfügung zu stellen, einschließlich der Herkunft von Materialien, Arbeitsbedingungen in der Lieferkette und der Einhaltung gesetzlicher Vorschriften.
- **Korrekte und vollständige Berichterstattung**: Alle Berichte, Dokumente und Informationen, die der REMSA GmbH bereitgestellt werden, müssen korrekt, vollständig und wahrheitsgemäß sein. Dies betrifft insbesondere finanzielle Berichte, Audit-Ergebnisse und Informationen zu Umwelt- und Sozialstandards.
- **Regelmäßige Berichterstattung**: Lieferanten müssen regelmäßig über ihre Fortschritte im Hinblick auf die Einhaltung der im Supplier Code of Conduct festgelegten Standards berichten. Dies kann durch regelmäßige Selbstbewertungen oder in Übereinstimmung mit den von der REMSA GmbH festgelegten Berichtspflichten erfolgen.

8.2. Audits und Überprüfung

Die REMSA GmbH behält sich das Recht vor, regelmäßige Audits oder Überprüfungen bei ihren Lieferanten durchzuführen, um die Einhaltung der Anforderungen dieses Supplier Code of Conduct zu gewährleisten:

- **Interne und externe Audits**: Lieferanten müssen bereit sein, sowohl interne als auch externe Audits zuzulassen. Diese Audits können unangekündigt stattfinden und sich auf verschiedene Bereiche konzentrieren, einschließlich Arbeitsbedingungen, Umweltschutzmaßnahmen, IT-Sicherheit und ethische Geschäftspraktiken.
- **Bereitstellung von Zugang**: Lieferanten müssen der REMSA GmbH und ihren Vertretern Zugang zu allen relevanten Geschäftsdaten, Dokumenten, Standorten und Produktionsstätten gewähren, die für eine ordnungsgemäße Prüfung erforderlich sind.
- **Kooperation bei Überprüfungen**: Lieferanten sind verpflichtet, uneingeschränkt mit den Auditoren zusammenzuarbeiten und alle angeforderten Informationen und Unterlagen rechtzeitig bereitzustellen.

8.3. Umgang mit Abweichungen

Sollten bei Audits, Berichten oder der täglichen Zusammenarbeit Abweichungen von den festgelegten Standards festgestellt werden, ist der Lieferant verpflichtet, diese Abweichungen unverzüglich zu beheben:

- **Meldung von Verstößen**: Wenn ein Lieferant feststellt, dass er gegen eine Anforderung dieses Supplier Code of Conduct verstoßen hat, muss er die REMSA GmbH unverzüglich informieren und geeignete Maßnahmen ergreifen, um den Verstoß zu beheben.
- **Korrekturmaßnahmen**: Nach Feststellung einer Abweichung ist der Lieferant verpflichtet, einen detaillierten Plan zur Korrektur der Probleme vorzulegen und die erforderlichen Maßnahmen umzusetzen. Die REMSA GmbH wird den Fortschritt überwachen und sicherstellen, dass die Maßnahmen ordnungsgemäß durchgeführt werden.
- **Folgen von Verstößen**: Schwerwiegende oder wiederholte Verstöße gegen die Anforderungen des Supplier Code of Conduct können zur Beendigung der Geschäftsbeziehung führen, falls keine ausreichenden Korrekturmaßnahmen getroffen werden.

8.4. Kommunikation und Zusammenarbeit

Eine offene Kommunikation und eine enge Zusammenarbeit zwischen der REMSA GmbH und ihren Lieferanten sind entscheidend, um gemeinsame Ziele zu erreichen und nachhaltige Geschäftsbeziehungen aufzubauen:

- **Regelmäßige Kommunikation**: Lieferanten müssen einen offenen und kontinuierlichen Dialog mit der REMSA GmbH pflegen. Probleme, Herausforderungen oder Änderungen in der Lieferkette müssen frühzeitig kommuniziert werden, um Verzögerungen oder Komplikationen zu vermeiden.
- **Engagement für kontinuierliche Verbesserung**: Lieferanten sollen sich aktiv an der kontinuierlichen Verbesserung von Geschäftsprozessen, Produkten und Dienstleistungen beteiligen. Dazu gehört auch die Bereitschaft, innovative Ansätze zu verfolgen und gemeinsam mit der REMSA GmbH an der Optimierung von Qualitäts- und Nachhaltigkeitsstandards zu arbeiten.
- **Zusammenarbeit in der Lieferkette**: Lieferanten müssen sicherstellen, dass sie mit ihren eigenen Unterlieferanten eng zusammenarbeiten, um die Einhaltung der im Supplier Code of Conduct festgelegten Standards zu gewährleisten. Dies umfasst regelmäßige Überprüfungen und die Kommunikation von Anforderungen an die gesamte Lieferkette.

8.5. Vertraulichkeit und Schutz von Informationen

Die REMSA GmbH verpflichtet sich, alle von den Lieferanten bereitgestellten Informationen vertraulich zu behandeln und erwartet dasselbe von ihren Lieferanten:

- **Vertraulicher Umgang mit Informationen**: Lieferanten müssen sicherstellen, dass vertrauliche Informationen der REMSA GmbH nicht an unbefugte Dritte weitergegeben werden. Dies gilt für alle geschäftlichen, technischen und personenbezogenen Daten.
- **Datenschutz und IT-Sicherheit**: Lieferanten müssen sicherstellen, dass alle Systeme, auf denen vertrauliche Informationen gespeichert sind, den höchsten Standards der IT-Sicherheit entsprechen, um unbefugten Zugriff oder Datenverlust zu verhindern.
- **Vertraulichkeitsvereinbarungen**: Lieferanten müssen sicherstellen, dass alle Mitarbeiter und Unterauftragnehmer, die Zugang zu vertraulichen Informationen haben, Vertraulichkeitsvereinbarungen unterzeichnet haben und die Bedeutung des Schutzes dieser Informationen verstehen.

Kapitel 9: Datensicherheit und Schutz von geistigem Eigentum

Die REMSA GmbH ist sich der hohen Bedeutung von Datensicherheit und dem Schutz von geistigem Eigentum bewusst. Diese Aspekte sind in der IT-Branche von entscheidender Bedeutung, um Vertrauen aufzubauen und langfristige, sichere Geschäftsbeziehungen zu gewährleisten. Unsere Lieferanten sind daher verpflichtet, höchste Standards in Bezug auf Datensicherheit und den Schutz von geistigem Eigentum zu erfüllen.

9.1. Verantwortung für Datensicherheit

Lieferanten der REMSA GmbH müssen sicherstellen, dass sie geeignete Maßnahmen ergreifen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten. Dies umfasst:

- **Sicherheitsrichtlinien und -verfahren**: Lieferanten müssen über formale Richtlinien und Verfahren zur Sicherstellung der IT-Sicherheit verfügen. Diese müssen regelmäßig aktualisiert werden, um auf neue Bedrohungen und Technologien zu reagieren.
- **Sicherheitsmanagementsystem**: Lieferanten sollten ein Sicherheitsmanagementsystem implementieren, das regelmäßig Audits und Sicherheitsüberprüfungen durchführt, um sicherzustellen, dass alle Systeme den geltenden Standards entsprechen.
- **Regelmäßige Schulungen**: Mitarbeiter der Lieferanten, die Zugang zu sensiblen Daten haben, müssen regelmäßig in den Bereichen IT-Sicherheit und Datenschutz geschult werden, um den sicheren Umgang mit diesen Informationen zu gewährleisten.

9.2. Schutz von Kundendaten

Die REMSA GmbH erwartet von ihren Lieferanten, dass sie alle Kundendaten sicher und vertraulich behandeln. Dies umfasst:

- **Datenschutzmaßnahmen**: Alle personenbezogenen Daten, die im Rahmen von Geschäftsbeziehungen verarbeitet werden, müssen gemäß den geltenden Datenschutzgesetzen (insbesondere der DSGVO) geschützt werden.
- **Vertrauliche Behandlung von Daten**: Lieferanten müssen sicherstellen, dass alle sensiblen und vertraulichen Daten, einschließlich Kundendaten, ausschließlich für die vertraglich festgelegten Zwecke verwendet und sicher gespeichert werden.
- **Zugriffsrechte**: Der Zugang zu sensiblen Daten muss streng kontrolliert werden, um sicherzustellen, dass nur autorisierte Personen Zugriff auf diese Informationen haben. Dies schließt den Einsatz von Rollen-basierter Zugriffskontrolle und der Mehrfaktor-Authentifizierung ein.

9.3. Schutz von geistigem Eigentum

Lieferanten müssen sicherstellen, dass sie die neuesten Sicherheitsstandards einhalten, um sich gegen Cyberangriffe und andere Sicherheitsbedrohungen zu schützen:

- **Erkennung und Reaktion auf Cyberangriffe**: Lieferanten müssen Mechanismen implementieren, um potenzielle Cyberangriffe frühzeitig zu erkennen und angemessen darauf zu reagieren. Dies umfasst den Einsatz von Firewalls, Intrusion Detection Systems (IDS) und anderen modernen Sicherheitstechnologien.

- **Schutz vor Datenlecks**: Lieferanten müssen Maßnahmen ergreifen, um sicherzustellen, dass keine unbefugten Zugriffe oder Datenlecks auftreten. Bei einem Sicherheitsvorfall muss die REMSA GmbH unverzüglich informiert werden.
- **Regelmäßige Sicherheitsüberprüfungen**: Lieferanten müssen regelmäßige Sicherheitsüberprüfungen und Penetrationstests durchführen, um potenzielle Schwachstellen in ihren IT-Systemen zu identifizieren und zu beheben.

9.4. Verantwortung im Umgang mit Cybersecurity-Bedrohungen

Lieferanten müssen sicherstellen, dass sie die neuesten Sicherheitsstandards einhalten, um sich gegen Cyberangriffe und andere Sicherheitsbedrohungen zu schützen:

- **Erkennung und Reaktion auf Cyberangriffe**: Lieferanten müssen Mechanismen implementieren, um potenzielle Cyberangriffe frühzeitig zu erkennen und angemessen darauf zu reagieren. Dies umfasst den Einsatz von Firewalls, Intrusion Detection Systems (IDS) und anderen modernen Sicherheitstechnologien.
- **Schutz vor Datenlecks**: Lieferanten müssen Maßnahmen ergreifen, um sicherzustellen, dass keine unbefugten Zugriffe oder Datenlecks auftreten. Bei einem Sicherheitsvorfall muss die REMSA GmbH unverzüglich informiert werden.
- **Regelmäßige Sicherheitsüberprüfungen**: Lieferanten müssen regelmäßige Sicherheitsüberprüfungen und Penetrationstests durchführen, um potenzielle Schwachstellen in ihren IT-Systemen zu identifizieren und zu beheben.

9.5. Maßnahmen zur Sicherstellung der Datenintegrität

Die REMSA GmbH erwartet, dass Lieferanten Mechanismen einrichten, die die Integrität von Daten sicherstellen:

- **Sicheres Backup und Wiederherstellung**: Lieferanten müssen regelmäßig Backups von wichtigen Daten erstellen und sicherstellen, dass im Falle eines Datenverlustes eine schnelle Wiederherstellung möglich ist.
- **Überprüfung von Datenzugriffen**: Alle Datenzugriffe müssen protokolliert und regelmäßig überprüft werden, um unbefugte Aktivitäten zu verhindern.
- **Datenverschlüsselung**: Lieferanten müssen sicherstellen, dass sensible Daten sowohl bei der Übertragung als auch im Ruhezustand verschlüsselt werden, um die Vertraulichkeit zu gewährleisten.

9.6. Sorgfaltspflichten gegenüber Dritten

Lieferanten, die Dritte in die Verarbeitung von Daten oder den Umgang mit geistigem Eigentum einbeziehen, müssen sicherstellen, dass diese Dritten ebenfalls die höchsten Standards der Datensicherheit und des Schutzes von geistigem Eigentum einhalten:

- **Vertragliche Sicherstellung**: Lieferanten müssen vertraglich sicherstellen, dass Dritte die gleichen Sicherheitsstandards wie sie selbst erfüllen. Dies umfasst insbesondere den Schutz sensibler Daten und die Vertraulichkeit von Geschäftsgeheimnissen.

- **Überwachung von Dritten**: Lieferanten müssen regelmäßig sicherstellen, dass ihre Unterauftragnehmer und Partner die vereinbarten Sicherheitsstandards einhalten. Dies kann durch regelmäßige Audits und Überprüfungen erfolgen.
- **Sorgfaltspflicht bei der Auswahl**: Lieferanten müssen bei der Auswahl von Dritten sicherstellen, dass diese über die notwendige Expertise und die technischen Voraussetzungen verfügen, um die Anforderungen an die Datensicherheit und den Schutz von geistigem Eigentum zu erfüllen.

9.7. Meldung von Sicherheitsvorfällen

Im Falle eines Sicherheitsvorfalls oder einer Verletzung des Schutzes von geistigem Eigentum muss der Lieferant die REMSA GmbH unverzüglich informieren:

- **Sofortige Benachrichtigung**: Jeder Vorfall, der zu einem Verlust oder einer Offenlegung von vertraulichen Daten oder geistigem Eigentum führt, muss innerhalb von 24 Stunden gemeldet werden.
- **Ergreifen von Maßnahmen**: Lieferanten müssen unverzüglich Maßnahmen zur Schadensbegrenzung ergreifen und einen Plan zur Behebung des Vorfalls und zur Verhinderung künftiger Sicherheitslücken vorlegen.
- **Untersuchung und Berichterstattung**: Lieferanten müssen eine gründliche Untersuchung des Vorfalls durchführen und der REMSA GmbH einen detaillierten Bericht über die Ursachen und die ergriffenen Maßnahmen zur Verfügung stellen.

Kapitel 10: Abweichungen und Sanktionen

Die REMSA GmbH ist bestrebt, langfristige, faire und vertrauensvolle Geschäftsbeziehungen mit ihren Lieferanten zu pflegen. Ein zentraler Bestandteil dieser Zusammenarbeit ist die Einhaltung der im Supplier Code of Conduct festgelegten Standards. Sollte ein Lieferant gegen diese Standards verstoßen oder Abweichungen festgestellt werden, behält sich die REMSA GmbH das Recht vor, angemessene Maßnahmen zu ergreifen, um die Einhaltung sicherzustellen. Dies kann von der Ergreifung von Korrekturmaßnahmen bis hin zur Beendigung der Geschäftsbeziehung reichen.

10.1. Meldung von Abweichungen

Lieferanten sind verpflichtet, jegliche Abweichungen von den im Supplier Code of Conduct festgelegten Standards oder Verstößen gegen Gesetze und Vorschriften unverzüglich der REMSA GmbH zu melden:

- **Selbstmeldung**: Lieferanten, die feststellen, dass sie gegen den Supplier Code of Conduct verstoßen haben, müssen diese Verstöße sofort melden und Maßnahmen zur Behebung ergreifen.
- **Meldung durch Dritte**: Sollten Dritte Verstöße gegen den Supplier Code of Conduct melden, wird die REMSA GmbH eine Untersuchung einleiten, um die Vorwürfe zu überprüfen und angemessene Maßnahmen zu ergreifen.

10.2. Untersuchung von Verstößen

Im Falle eines gemeldeten oder vermuteten Verstoßes gegen die im Supplier Code of Conduct festgelegten Standards wird die REMSA GmbH eine Untersuchung einleiten:

- **Untersuchungsverfahren**: Lieferanten müssen uneingeschränkt mit der REMSA GmbH und deren Vertretern bei der Untersuchung von Verstößen zusammenarbeiten. Dies umfasst die Bereitstellung von Informationen, die Zugangsgewährung zu Standorten und die Offenlegung von relevanten Dokumenten.
- **Überprüfung der Fakten**: Die REMSA GmbH wird alle Fakten in Bezug auf den gemeldeten Verstoß prüfen und in Zusammenarbeit mit dem Lieferanten die Ursachen und Verantwortlichkeiten klären.
- **Transparente Kommunikation**: Lieferanten müssen in diesem Prozess transparent und kooperativ sein, um sicherzustellen, dass Verstöße schnell und effektiv aufgeklärt werden können.

10.3. Korrekturmaßnahmen

Sollte ein Verstoß festgestellt werden, erwartet die REMSA GmbH, dass der Lieferant unverzüglich Korrekturmaßnahmen ergreift:

- **Entwicklung eines Korrekturplans**: Der Lieferant muss einen detaillierten Plan vorlegen, der beschreibt, wie der Verstoß behoben wird und welche Maßnahmen ergriffen werden, um zukünftige Verstöße zu verhindern.
- **Fristen für Korrekturmaßnahmen**: Der Lieferant muss alle Korrekturmaßnahmen innerhalb eines angemessenen Zeitrahmens umsetzen, der in Absprache mit der REMSA GmbH festgelegt wird.
- **Nachverfolgung**: Die REMSA GmbH wird den Fortschritt der Korrekturmaßnahmen überwachen und sicherstellen, dass alle erforderlichen Schritte durchgeführt werden, um die Einhaltung des Supplier Code of Conduct wiederherzustellen.

10.4. Sanktionen bei Nichtbehebung von Verstößen

Sollte ein Lieferant die festgelegten Korrekturmaßnahmen nicht umsetzen oder schwerwiegende Verstöße begehen, behält sich die REMSA GmbH das Recht vor, Sanktionen zu verhängen:

- **Vertragsstrafen**: In bestimmten Fällen können Vertragsstrafen verhängt werden, um die Nichteinhaltung des Supplier Code of Conduct zu ahnden.
- **Reduzierung von Aufträgen**: Die REMSA GmbH kann beschließen, das Auftragsvolumen eines Lieferanten zu reduzieren, bis die Verstöße vollständig behoben wurden.
- **Suspendierung der Zusammenarbeit**: In schwerwiegenden Fällen kann die REMSA GmbH die Geschäftsbeziehung mit einem Lieferanten vorübergehend aussetzen, bis alle Korrekturmaßnahmen abgeschlossen sind.
- **Beendigung der Geschäftsbeziehung**: Wenn ein Lieferant wiederholt gegen den Supplier Code of Conduct verstößt oder schwerwiegende ethische, gesetzliche oder vertragliche Verstöße begeht, behält sich die REMSA GmbH das Recht vor, die Geschäftsbeziehung dauerhaft zu beenden.

10.5. Eskalationsverfahren

Sollte ein Lieferant den Korrekturmaßnahmen oder Sanktionen nicht zustimmen oder es zu Meinungsverschiedenheiten kommen, kann ein Eskalationsverfahren eingeleitet werden:

- **Verhandlungen**: Beide Parteien können versuchen, durch Verhandlungen eine einvernehmliche Lösung zu finden, um die Situation zu klären.
- **Mediation**: Falls erforderlich, kann eine Mediation oder Schlichtung durch unabhängige Dritte erfolgen, um eine neutrale Lösung herbeizuführen.
- **Gerichtliche Schritte**: In Fällen, in denen keine Einigung erzielt werden kann und die Verstöße schwerwiegend sind, behält sich die REMSA GmbH das Recht vor, gerichtliche Schritte einzuleiten.

10.6. Dokumentation und Benachrichtigung

Lieferanten müssen die Einhaltung des Supplier Code of Conduct regelmäßig dokumentieren und sicherstellen, dass Abweichungen und Korrekturmaßnahmen ordnungsgemäß festgehalten werden:

- **Regelmäßige Selbstbewertungen**: Lieferanten sollten regelmäßig interne Selbstbewertungen durchführen, um sicherzustellen, dass sie den Anforderungen des Supplier Code of Conduct entsprechen.
- **Berichterstattung über Korrekturmaßnahmen**: Lieferanten müssen die REMSA GmbH regelmäßig über den Status und die Ergebnisse der Korrekturmaßnahmen informieren, um sicherzustellen, dass die Einhaltung wiederhergestellt wird.
- **Nachhaltige Verbesserung**: Lieferanten sollten nicht nur kurzfristige Korrekturen umsetzen, sondern auch Maßnahmen zur nachhaltigen Verbesserung einführen, um ähnliche Verstöße in der Zukunft zu verhindern.