



Der Leiter der Rechtsabteilung

Internationales Compliance- Programm

Dokumenttyp:

Richtlinie

ID: Nr. 56_v.2

Geltungsbereich:

Gruppe

Prozess:

Internes Kontroll- und
Risikomanagementsystem/C
ompliance und Modell 231

Datum: 30.06.2025



INHALTSVERZEICHNIS

<i>EINLEITUNG</i>	<i>4</i>
<i>ZWECK</i>	<i>5</i>
<i>AUFGABEN UND VERANTWORTLICHKEITEN</i>	<i>8</i>
<i>BEREICHE DER COMPLIANCE</i>	<i>9</i>
<i>ÜBERWACHUNG</i>	<i>9</i>
<i>BERICHTERSTATTUNG</i>	<i>10</i>
<i>SCHULUNG UND KOMMUNIKATION</i>	<i>10</i>
<i>DISZIPLINARISCHES SYSTEM UND VERTRAGLICHE RECHTSMITTEL</i>	<i>11</i>
<i>ANHANG – ALLGEMEINE KONTROLLSTANDARDS, RISIKOBEREICHE UND SPEZIFISCHE VERHALTENSSTANDARDS</i>	<i>15</i>



HAFTUNGSAUSSCHLUSS

Die in diesem Dokument definierten Grundsätze und Verhaltensregeln stellen auch Kontrollmaßnahmen zur Korruptionsbekämpfung und zur Prävention von Kriminalitätsrisiken gemäß dem italienischen Gesetzesdekret 231/2001 dar. Sie stehen im Einklang mit den Bestimmungen des von der Gesellschaft gemäß dem italienischen Gesetzesdekret 231/2001 (Modell 231) verabschiedeten Organisations-, Verwaltungs- und Kontrollmodells Ethikkodex der FS Italiane Group, Antikorruptionsrichtlinie und Antikorruptions-Managementmodell ¹, Datenschutzrahmenwerk und Klassifizierungs- und Vertraulichkeitsschutzrahmenwerk der FS Italiane Group.

Den Leitern der beteiligten Strukturen wird empfohlen, dieses Dokument ständig zu überwachen, um seine korrekte Anwendung und ständige Anpassung im Hinblick auf seine Wirksamkeit sicherzustellen. Jeder, der Kenntnis von einem Verstoß oder einer versuchten Umgehung dieses Dokuments erhält, muss unverzüglich den Aufsichtsrat und/oder den Ethik- und Berichtsausschuss des Unternehmens gemäß den im Whistleblowing-Managementverfahren und im Modell 231 festgelegten Verfahren informieren.

KONTROLLMASSNAHMEN

- ☒ Italienisches Gesetzesdekret 231/2001
- ☒ zur Korruptionsbekämpfung

Die in diesem Dokument enthaltenen Bestimmungen stehen im Einklang mit denen des Governance-Modells der FS Italiane Group und der Konzernordnung. Sollte sich eine hierin enthaltene Angelegenheit auf Themen beziehen, die für Angelegenheiten relevant und/oder funktional sind, die nicht in den Zuständigkeitsbereich der Holding fallen, so hat die ausschließliche Zuständigkeit der jeweiligen Konzerngesellschaft Vorrang.

¹ Soweit vom Unternehmen übernommen. Das Modell wurde in seiner ersten Fassung unter dem Namen „Anti-Bribery & Corruption Management System“ (Konzernrichtlinie Nr. 247 P/AD vom 23.02.2018 und entsprechende Unternehmensdokumente) veröffentlicht. Entsprechend ihren besonderen Merkmalen haben Anas SpA und QMU SpA ein eigenes freiwilliges Organisations- und Managementmodell zur Korruptionsbekämpfung und Transparenz eingeführt.

EINLEITUNG

Die FS Italiane Group (im Folgenden auch als FS Group bezeichnet) verfügt über eine konsolidierte Stellung auf internationaler Ebene, die durch das direkte Engagement ihrer ausländischen Tochtergesellschaften gewährleistet wird, die in unterschiedlichen und sich ergänzenden Sektoren/Märkten tätig sind.

In den letzten Jahren haben viele Länder, in denen die FS Group tätig ist, ein Haftungssystem für juristische Personen in Bezug auf rechtswidrige Handlungen von Vertretern, Mitarbeitenden oder Dritten, die in ihrem Interesse handeln, eingeführt. Die meisten dieser Vorschriften ermutigen Unternehmen, Corporate-Governance-Strukturen und Risikopräventionssysteme einzuführen, wobei sie in einigen Fällen eine Befreiung oder Milderung der geltenden Sanktionen vorsehen, wenn geeignete Präventivmaßnahmen getroffen wurden.

In diesem Zusammenhang bekräftigt die FS Group ihr Engagement für die Prävention und Bekämpfung rechtswidriger Aktivitäten in ihrem Geschäftsbetrieb.

Dieses Dokument dient als Grundlage für die Stärkung des internen Kontroll- und Risikomanagementsystems auf Konzernebene in Übereinstimmung mit den wichtigsten und aktuellsten Best Practices und Vorschriften zu Compliance-Programmen², um die angewandten Grundsätze zu harmonisieren und einen gemeinsamen, einheitlichen und umfassenden Ansatz gegen rechtswidriges oder umgehendes Verhalten zu schaffen.

² Beispiele hierfür sind unter anderem die folgenden:

- das italienische Gesetzesdekret Nr. 231 vom 8. Juni 2001 in seiner geänderten Fassung, das die administrative Haftung (ähnlich der strafrechtlichen Haftung) juristischer Personen regelt, die sich aus der Begehung bestimmter Straftaten in ihrem Interesse oder zu ihrem Vorteil ergibt;
- der von der Borsa Italiana S.p.A. geförderte „Corporate Governance Code“ für börsennotierte Unternehmen;
- das „Federal Sentencing Guidelines Manual & Supplement“ (Handbuch und Ergänzung zu den bundesstaatlichen Strafzumessungsrichtlinien), verabschiedet von der United States Sentencing Commission (US-Strafzumessungskommission) am 1. November 2010;
- das „Foreign Corruption Practice Act“ („FCPA“) von 1977 in seiner geänderten Fassung;
- das „UK Bribery Act“ von 2010 in seiner geänderten Fassung;
- die vom OECD-Rat am 18. Februar 2010 verabschiedeten „Good Practice Guidance on Internal Controls, Ethics, and Compliance“ (Leitlinien für bewährte Praktiken in den Bereichen interne Kontrollen, Ethik und Compliance);
- der „Leitfaden zum US-Gesetz über Korruptionspraktiken im Ausland“ (Resource Guide to the U.S. Foreign Corrupt Practices Act), herausgegeben von der Strafrechtsabteilung des US-Justizministeriums (Department of Justice, DOJ) und der Vollstreckungsabteilung der US-Börsenaufsichtsbehörde (Securities and Exchange Commission) im Jahr 2012, in der jeweils gültigen Fassung;
- die „Evaluation of Corporate Compliance Programs“ (Bewertung von Compliance-Programmen für Unternehmen) des DOJ aus dem Jahr 2017 in ihrer jeweils gültigen Fassung;
- das „Anti-Corruption Ethics and Compliance Programme for Business: A Practical Guide“ (Ethik- und Compliance-Programm zur Korruptionsbekämpfung für Unternehmen: Ein praktischer Leitfaden), das im September 2013 vom Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung („UNODC“) verabschiedet wurde;
- die Empfehlungen der Financial Action Task Force („FATF-GAFT“ oder „GAFT“) zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung aus dem Jahr 2012 in ihrer geänderten Fassung;
- Europäische Verordnungen über Geldwäsche, die Ermittlung, Beschlagnahme und Einziehung von Erträgen aus Straftaten und über die Terrorismusfinanzierung (einschließlich der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 und der Delegierten Verordnung (EU) 2016/1675 in ihrer geänderten Fassung).

ZWECK

Das internationale Compliance-Programm bietet die Möglichkeit, das interne Kontroll- und Risikomanagementsystem zu stärken, und soll ein Verhalten fördern, das auf den Grundsätzen der Loyalität, Fairness, Ehrlichkeit, Integrität und Einhaltung von Gesetzen, Vorschriften, Standards und bewährten Verfahren basiert.

Das internationale Compliance-Programm zielt darauf ab, Compliance-Risiken zu vermeiden, d. h. Verstöße gegen nationale oder internationale (gesetzliche oder regulatorische) oder selbstregulatorische Vorschriften (z. B. Statuten, Verhaltenskodizes, Selbstregulierungskodizes) zu verhindern, die neben Reputationsschäden auch zu Sanktionen durch nationale, ausländische oder supranationale Justiz- oder Verwaltungsbehörden führen können, einschließlich restriktiver und disqualifizierender Maßnahmen (z. B. Aussetzung oder Einstellung der Tätigkeit, Verbot von Verträgen mit der öffentlichen Verwaltung, Aufnahme in schwarze Listen, Disqualifizierung usw.), die die Geschäftskontinuität gefährden und erhebliche wirtschaftliche und finanzielle Verluste verursachen können.

In diesem Zusammenhang werden im Internationalen Compliance-Programm allgemeine Kontrollstandards, Compliance-Bereiche, Risikobereiche und spezifische Verhaltensstandards festgelegt, um den Adressaten einen einheitlichen Regelkatalog zur Verfügung zu stellen, der darauf abzielt, die Haftung des Unternehmens zu verhindern.

Alle ausländischen Unternehmen sind allein dafür verantwortlich, das Risiko von Straftaten innerhalb ihrer Organisation zu verhindern.

Alle ausländischen Unternehmen sind verpflichtet, im erforderlichen und angemessenen Umfang Kontrollmaßnahmen einzuführen sowie die in diesem Dokument dargelegten Grundsätze und Hinweise zu ergänzen, zu übernehmen oder weiterzuentwickeln.

Darüber hinaus sind alle ausländischen Unternehmen in jedem Fall verpflichtet, weitere Compliance-Bereiche, Risikobereiche und spezifische Verhaltensstandards zu identifizieren, die ihrem eigenen Betriebskontext und den lokalen Referenzvorschriften zuzuordnen sind, und gegebenenfalls weitere Präventions- und Kontrollinstrumente einzuführen, um den identifizierten spezifischen Risiken zu begegnen, auch in Umsetzung der Vorschriften der Gruppe.

Die Bestimmungen des Internationalen Compliance-Programms werden durch die folgenden Bestimmungen ergänzt:

- der Verhaltenskodex der Gruppe;
- die Antikorruptionsrichtlinie der Gruppe und die Modelle für das Antikorruptionsmanagement des Unternehmens;
- die Sanktionsrichtlinie der Gruppe;
- das Kartellrechts-Compliance-Programm der Gruppe;
- das Datenschutz-Rahmenwerk der Gruppe;
- die Steuerstrategie der Gruppe;
- die Regeln für die interne Verwaltung und externe Kommunikation von Insiderinformationen und für den Umgang mit vertraulichen Informationen;

- das interne Kontroll- und Risikomanagementmodell der Ferrovie dello Stato Italiane-Gruppe für die Finanzberichterstattung;
- die Unternehmens- und Konzernrichtlinien, Verfahren und Organisationsdokumente.

ANWENDUNGSBEREICH

- Ferrovie dello Stato Italiane SpA
- FS International SpA und FS Logistix SpA
- Ausländische Unternehmen, die zur FS Italiane Group gehören³

LEITUNG UND KOORDINIERUNG**VERFAHREN ZUR ANNAHME DURCH DAS UNTERNEHMEN**

Dieses Dokument ist eine Leitungs- und Koordinierungsmaßnahme.

In Übereinstimmung mit ihren Vorrechten der Autonomie und Unabhängigkeit verabschieden FS International SpA, FS Logistix und die ausländischen Tochtergesellschaften⁴ dieses Dokument und gewährleisten die korrekte und konsequente Anwendung der darin festgelegten Bestimmungen, deren maximale interne Verbreitung und die entsprechende Umsetzungskontrolle unter Einhaltung der Vertraulichkeitsverpflichtungen und der Vorrechte der Autonomie und Unabhängigkeit jedes Unternehmens.



Direkte Anwendbarkeit

³ Ausländische Unternehmen der FS Italiane Group sind ausländische Unternehmen, die gemäß Artikel 2359(1)(1,2) des italienischen Zivilgesetzbuches von FS SpA kontrolliert werden.

⁴ Die ausländischen Unternehmen wenden die regulierten Grundsätze in Übereinstimmung mit dem für den Sitz des Unternehmens geltenden Rechtssystem an.

ROLLEN UND VERANTWORTLICHKEITEN

FS SpA Compliance-Struktur

Die Compliance-Struktur der FS SpA gewährleistet:

- die Erstellung und Aktualisierung des internationalen Compliance-Programms;
- die Förderung geeigneter und spezifischer Informations- und Kommunikationskampagnen in Zusammenarbeit mit den zuständigen Unternehmensstrukturen, um die Kenntnis des internationalen Compliance-Programms sicherzustellen, mit Unterstützung der **Personalabteilung von FS International SpA**;
- die regelmäßige Unterrichtung der Geschäftsleitung und der Kontrollorgane über die Umsetzung des Internationalen Compliance-Programms mit Unterstützung der **Personalabteilung von FS International SpA**.

Personalabteilung von FS International SpA

Personalabteilung von FS International SpA:

- überwacht den Stand der Umsetzung des internationalen Compliance-Programms durch die ausländischen Unternehmen und arbeitet dabei mit den zuständigen Unternehmensstrukturen zusammen;
- unterstützt die **Compliance-Struktur von FS SpA** bei der regelmäßigen Information der Geschäftsleitung und der Kontrollorgane über die Umsetzung des internationalen Compliance-Programms;
- unterstützt die **Compliance-Struktur von FS SpA** und die zuständigen Unternehmensstrukturen bei der Förderung geeigneter und spezifischer Informations- und Kommunikationskampagnen, die darauf abzielen, das Bewusstsein für das internationale Compliance-Programm zu schärfen.

Compliance-Struktur ausländischer Unternehmen (oder Focal Point Compliance)

In Bezug auf den betrieblichen Kontext und in Übereinstimmung mit den einschlägigen lokalen Vorschriften ist die Compliance-Struktur jedes ausländischen Unternehmens (oder Focal Point Compliance) verantwortlich für:

- die Bewertung der Angemessenheit des internationalen Compliance-Programms in Bezug auf das Geschäftsumfeld und die einschlägigen lokalen Vorschriften;
- die Identifizierung weiterer Compliance-Bereiche, Risikobereiche und/oder spezifischer Verhaltensstandards sowie die Bewertung der Einführung/Aktualisierung weiterer Präventions- und Kontrollinstrumente zur Bewältigung der identifizierten spezifischen Risiken, auch im Rahmen der Umsetzung von Konzernvorschriften;
- die Unterstützung der zuständigen Unternehmensstrukturen bei der Definition und/oder Aktualisierung der internen Regulierungsdokumente in Bezug auf die Compliance-Bereiche;

- die Förderung geeigneter und spezifischer Schulungs-, Informations- und Kommunikationskampagnen zur Sensibilisierung für das internationale Compliance-Programm durch Zusammenarbeit mit den zuständigen Unternehmensstrukturen;
- die Sicherstellung, dass regelmäßig über den Fortschritt des internationalen Compliance Programms berichtet wird, im Rahmen der regelmäßigen Informationsflüsse an die oberste Führungsebene und an die Kontrollorgane, wie im Compliance Modell der Gruppe vorgesehen.

COMPLIANCE-BEREICHE

Der Geltungsbereich des Dokuments umfasst die folgenden Compliance-Bereiche:

- a) Korruptionsdelikte;
- b) sonstige Straftaten gegen die öffentliche Verwaltung;
- c) Bilanzfälschung;
- d) Steuerdelikte;
- e) Organisierte Kriminalität;
- f) Finanzierung des Terrorismus und sogenannte Geldwäschedelikte;
- g) Marktmissbrauch;
- h) Straftaten gegen Personen;
- i) Verbrechen gegen Gesundheit und Sicherheit;
- j) Umweltdelikte;
- k) Computerkriminalität;
- l) Urheberrechtsverstöße;
- m) Schmuggel;
- n) Verbrechen gegen das kulturelle Erbe.

Die Liste der Compliance-Bereiche sowie der Risikobereiche und die damit verbundenen spezifischen Verhaltensstandards, die im beigefügten Dokument aufgeführt sind, bilden den Ausgangspunkt für ausländische Unternehmen, um ihre eigene Bewertung des Betriebskontextes und der lokalen Vorschriften durchzuführen, mit dem Ziel, zusätzliche Compliance-Bereiche, Risikobereiche und/oder spezifische Verhaltensstandards zu identifizieren (Risikobewertung) und die Einführung/Aktualisierung von Organisationsdokumenten zu bewerten (Lückenanalyse).

ÜBERWACHUNG

Die Compliance-Strukturen der ausländischen Unternehmen (oder Focal Point Compliance) sind für die Überwachung der Angemessenheit und Einhaltung des internationalen Compliance-Programms verantwortlich. Basierend auf dem operativen Kontext

und in Übereinstimmung mit den einschlägigen lokalen Vorschriften sind sie verantwortlich für:

- die Angemessenheit des internationalen Compliance-Programms zu bewerten;
- die Identifizierung zusätzlicher Compliance-Bereiche, Risikobereiche und/oder spezifischer Verhaltensstandards sowie Bewertung der Einführung/Aktualisierung zusätzlicher Organisationsdokumente zur Bewältigung der identifizierten spezifischen Risiken;
- die Unterstützung der zuständigen Unternehmensstrukturen bei der Definition und/oder Aktualisierung der Organisationsdokumente in Bezug auf die Compliance-Bereiche.

Darüber hinaus überwacht die **Personalabteilung von FS International SpA** den Stand der Umsetzung des internationalen Compliance-Programms durch die ausländischen Unternehmen in Zusammenarbeit mit den zuständigen Unternehmensstrukturen.

BERICHTERSTATTUNG

Im Rahmen des regelmäßigen Informationsflusses, der im Compliance-Modell der Gruppe vorgesehen ist, informiert die Compliance-Struktur der ausländischen Unternehmen (oder Focal Point Compliance) die oberste Geschäftsleitung und die Kontrollorgane über den Stand der Umsetzung des internationalen Compliance-Programms.

Darüber hinaus informiert die **Compliance-Struktur von FS SpA** mit Unterstützung der **Personalabteilung von FS International SpA** die Geschäftsleitung und die Kontrollorgane von FS regelmäßig über die Umsetzung des internationalen Compliance-Programms innerhalb der Gruppe im Rahmen der im Compliance-Modell der Gruppe vorgesehenen regelmäßigen Informationsflüsse.

SCHULUNG UND KOMMUNIKATION

Die FS SpA und alle ausländischen Unternehmen fördern das Bewusstsein für den Inhalt des internationalen Compliance-Programms.

Alle ausländischen Unternehmen planen und verwalten die Schulungsmaßnahmen zu den Inhalten des internationalen Compliance-Programms und/oder der zusätzlichen Präventions- und Kontrollinstrumente, die zur Bewältigung spezifischer identifizierter Risiken vorgesehen sein können, und überwachen die Teilnahme aller betroffenen Mitarbeitenden an den geplanten Schulungen.

In Übereinstimmung mit den neuesten Best Practices müssen die Schulungen „auf realen Szenarien basieren“, d. h. sie müssen sich auf praktische Fälle beziehen, in denen die allgemeinen Kontrollstandards und spezifischen Verhaltensstandards innerhalb jedes Risikobereichs verletzt werden könnten, und mögliche Verhaltensweisen aufzeigen, mit denen die Einhaltung des internationalen Compliance-Programms sichergestellt werden kann, sowie Anweisungen zur Erkennung und zum Umgang mit potenziellen Warnsignalen enthalten.

Die Teilnahme an Schulungsmaßnahmen ist obligatorisch.

Um eine maximale Verbreitung der Inhalte des internationalen Compliance-Programms und die Wirksamkeit der darin enthaltenen Verhaltensregeln und Präventivmaßnahmen zu gewährleisten, muss das internationale Compliance-Programm über interne (Intranet des Unternehmens) und externe (Website) Kommunikationskanäle zugänglich gemacht werden.

Die Grundsätze und Inhalte dieses Dokuments werden Dritten durch Vertragsklauseln zur Kenntnis gebracht, die die Vertragspartei auf der Grundlage der vertraglich geregelten Tätigkeit zur Einhaltung der für sie unmittelbar geltenden Bestimmungen verpflichten.

DISZIPLINARSYSTEM UND VERTRAGLICHE RECHTSBEHELFE

Verstöße gegen das internationale Compliance-Programm durch Mitarbeiter von Konzernunternehmen können zu Disziplinarmaßnahmen gemäß den von jedem Unternehmen festgelegten Maßnahmen führen.

Verstöße Dritter gegen die Grundsätze oder Bestimmungen des internationalen Compliance-Programms können auf der Grundlage spezifischer Bewertungen durch das betreffende Konzernunternehmen zur Nichtbegründung oder Beendigung von Vertragsbeziehungen führen.

Unterzeichnet von
Mario Antonio Scino

GLOSSAR

Risikobereich: Bereiche/Aktivitäten, in denen das Risiko der Begehung der in den Compliance-Bereichen identifizierten Verstöße genauer betrachtet werden kann.

Compliance-Bereiche: Kategorien von Straftaten, deren Verhinderung in der FS-Gruppe Vorrang haben sollte, um ihre Geschäfte mit Ehrlichkeit und Integrität zu führen.

Ausländische Tochtergesellschaft oder ausländisches Unternehmen: Ausländische Unternehmen, die gemäß Artikel 2359(1)(1,2) des italienischen Zivilgesetzbuches von FS SpA kontrolliert werden.

FS Italiane Group oder FS Group oder Gruppe: FS und ihre Tochtergesellschaften im Sinne von Artikel 2359 des italienischen Zivilgesetzbuches.

FS SpA oder Holdinggesellschaft: Ferrovie dello Stato Italiane SpA.

Allgemeine Kontrollstandards: Allgemeine Kontrollstandards, die von jeder ausländischen Tochtergesellschaft anzuwenden sind, um eine solide, ordnungsgemäße und kohärente Geschäftsführung zu gewährleisten.

Empfänger: Mitglieder der Unternehmensorgane und des Aufsichtsrats, Mitarbeiter und alle Arten von Mitarbeitern der ausländischen Unternehmen der FS-Gruppe und Dritte.

Spezifische Verhaltensstandards: Mindeststandards für das Verhalten, das alle ausländischen Tochtergesellschaften in Bezug auf jeden Risikobereich einhalten müssen.

Dritte: alle Personen, die vertragliche Beziehungen zu ausländischen Unternehmen der FS-Gruppe unterhalten (z. B. Lieferanten, Geschäftspartner, Berater und Handelsförderer, Wirtschaftsprüfer usw.), unabhängig davon, ob diese Beziehungen vorübergehender oder dauerhafter Natur sind.



ANHANG 1 – ORGANISATORISCHE REFERENZEN

ROLLE	DATUM	ORGANISATIONSTRUKTUR	REFERENZDOKUMENT
Compliance-Struktur der FS SpA	30.06.2025	Compliance-Struktur innerhalb DER RECHTSABTEILUNG	DOr Nr. 153/LEG-COA vom 08.10.2021
Personalstruktur von FS International SpA	30.06.2025	Personalstruktur, direkt der Geschäftsführung unterstellt	DOr Nr. 10/AU vom 01.05.2025
Organisationsstruktur	30.06.2025	GRUPPENORGANISATION innerhalb von PEOPLE, CULTURE & TRANSFORMATION	DOr Nr. 150/AD vom 16.04.2025

RECHTLICHE HINWEISE

- Ethikkodex der Gruppe;
- Rechts- und Compliance-Governance-Modell;
- Compliance-Modell der FS Italiane Group;
- Konzernrichtlinie zur Korruptionsbekämpfung und Modelle zum Management der Korruptionsbekämpfung im Unternehmen;
- Datenschutzrahmen der Gruppe;
- Sanktionsrichtlinie der Gruppe;
- Kartellrechts-Compliance-Programm der Gruppe;
- Steuerstrategie der Ferrovie dello Stato Italiane Group;
- Regeln für die interne Verwaltung und externe Kommunikation von Insiderinformationen und für den Umgang mit vertraulichen Informationen;
- Modell der Ferrovie dello Stato Italiane-Gruppe für die interne Kontrolle und das Risikomanagement im Bereich der Finanzberichterstattung.

ANHANG – ALLGEMEINE KONTROLLSTANDARDS, RISIKOBEREICHE UND SPEZIFISCHE VERHALTENSSTANDARDS

Beigefügtes Dokument⁵, in dem für jeden Bereich der Einhaltung im Geltungsbereich des Dokuments die allgemeinen Kontrollstandards, die Risikobereiche und die spezifischen Verhaltensstandards aufgeführt sind, die jedes ausländische Unternehmen einhalten muss.

⁵ Der Anhang, der integraler Bestandteil dieses Dokuments ist, wird im Falle späterer regulatorischer Änderungen und/oder aufgrund betrieblicher Erfordernisse von der [Compliance-Struktur der FS SpA](#) mit Unterstützung der [Organisationsstruktur der FS SpA](#) aktualisiert und im Intranet des Unternehmens im Bereich für Organisationsdokumente zur Verfügung gestellt, ohne dass dieses Dokument neu herausgegeben werden muss.



DOKUMENTVERSIONIE RUN G

VERSION/DATUM	DOKUMENT	GRUND FÜR DIE ÜBERARBEITUNG
1.0 vom 19.12.2023	<i>GR_PY_Internationales Compliance-Programm _n.56_V.02</i>	Erste Ausgabe
2.0 vom 30.06.2025	<i>GR_PY_Internationales Compliance-Programm _n.56_V.02</i>	Zweite Ausgabe – Überprüfung der Rollen und Verantwortlichkeiten in Bezug auf Überwachungs- und Berichterstattungsaktivitäten und Anpassung an das neue Governance-Modell der Gruppe

Der Leiter der Rechtsabteilung

„Internationales Compliance-Programm“ Konzernrichtlinie

Anhang „Allgemeine Kontrollstandards, Risikobereiche und spezifische Verhaltensstandards“

INHALTSVERZEICHNIS

EINLEITUNG	3
ALLGEMEINE KONTROLLSTANDARDS	3
RISIKOBEREICHE UND SPEZIFISCHE VERHALTENSSTANDARDS	4
KORRUPTIONSVERBRECHEN	4
SONSTIGE STRAFTATEN GEGEN DIE ÖFFENTLICHE VERWALTUNG	4
BILANZFÄLSCHUNG	5
STEUERSTRAFTATEN	7
ORGANISIERTE KRIMINALITÄT	8
FINANZIERUNG VON TERRORISMUS UND SOGENANNT E GELDWÄSCHE	9
MARKTMISSBRAUCH	11
STRAFTATEN GEGEN PERSONEN	12
STRAFTATEN GEGEN GESUNDHEIT UND SICHERHEIT	13
UMWELTSTRAFTATEN	15
COMPUTERVERBRECHEN	16
URHEBERRECHTSVERSTÖSSE	18
SCHMUGGEL	19
VERBRECHEN GEGEN DAS KULTURELLE ERBE	19



EINLEITUNG

Dieses Dokument enthält die allgemeinen Kontrollstandards, die Risikobereiche sowie die spezifischen Verhaltensstandards für jeden im Rahmen des internationalen Compliance-Programms identifizierten Compliance-Bereich, wie nachstehend aufgeführt:

- a) Korruptionsdelikte;
- b) Sonstige Straftaten gegen die öffentliche Verwaltung;
- c) Bilanzfälschung;
- d) Steuerdelikte;
- e) Organisierte Kriminalität;
- f) Finanzierung des Terrorismus und sogenannte Geldwäschedelikte;
- g) Marktmissbrauch;
- h) Straftaten gegen Personen;
- i) Straftaten gegen Gesundheit und Sicherheit;
- j) Umweltdelikte;
- k) Computerkriminalität;
- l) Urheberrechtsverstöße;
- m) Schmuggel;
- n) Verbrechen gegen das kulturelle Erbe.

ALLGEMEINE KONTROLLSTANDARDS

Die nachstehend aufgeführten allgemeinen Kontrollstandards gelten allgemein für alle Compliance-Bereiche, und jedes ausländische Unternehmen ist zu ihrer Einhaltung verpflichtet:

- *Trennung von Aufgaben und Verantwortlichkeiten:* Sicherstellung der Trennung von Aufgaben zwischen den ausführenden, kontrollierenden und/oder genehmigenden Personen, auch durch die Erstellung von Benutzerprofilen innerhalb der IT-Systeme, entsprechend den übertragenen und stellvertretenden Befugnissen;
- *Rollen und Verantwortlichkeiten:* Formalisierung interner Vorschriften, in denen Aufgaben, Verantwortlichkeiten und operative Methoden für die Durchführung relevanter/operativer Tätigkeiten beschrieben werden;
- *System der delegierten und stellvertretenden Befugnisse:* Festlegung eines Systems der delegierten und stellvertretenden Befugnisse, das entsprechend der organisatorischen Position und der Hierarchieebene der Empfänger den Grad der Autonomie, die Vertretungsbefugnisse und die zugewiesenen Ausgabengrenzen festlegt;

- *Rückverfolgbarkeit und Aufbewahrung:* Gewährleistung der Rückverfolgbarkeit und Überprüfbarkeit von Aktivitäten und Kontrollen durch geeignete dokumentarische und/oder IT-Unterstützung sowie deren Aufbewahrung in Übereinstimmung mit den geltenden Vorschriften und Richtlinien der Gruppe;
- *Unparteilichkeit und Vermeidung von Interessenkonflikten:* Sicherstellung, dass die Personen, die in den in diesem Dokument beschriebenen Risikobereichen tätig sind, professionell und unparteiisch handeln, die geltenden Gesetze und Vorschriften einhalten und Situationen, aus denen sich ein Interessenkonflikt ergeben könnte, vermeiden und unverzüglich melden;
- *Korrekte Gestaltung der Beziehungen zu Dritten:* In den Beziehungen zu Dritten ist gemäß einem risikobasierten Ansatz Folgendes sicherzustellen:
 - (i) Überprüfung der Zuverlässigkeit, Reputation und Eignung von Dritten, mit denen jedes ausländische Unternehmen eine berufliche und geschäftliche Beziehung aufbauen möchte;
 - (ii) Bereitstellung spezifischer vertraglicher Anweisungen, die Dritte zur Einhaltung der in diesem internationalen Compliance-Programm enthaltenen Grundsätze verpflichten;
 - (iii) Überprüfung der erbrachten Leistungen und der Angemessenheit der auszahlenden Beträge.

RISIKOBEREICHE UND SPEZIFISCHE VERHALTENSSTANDARDS

Nachstehend sind die Risikobereiche und spezifischen Verhaltensstandards aufgeführt, die jedes ausländische Unternehmen für jeden Compliance-Bereich einhalten muss.

KORRUPTIONSDELIKTE

Die Definition von Korruptionsdelikten, die Identifizierung von Risikobereichen und spezifische Verhaltensstandards finden Sie in der Antikorruptionsrichtlinie der FS Group.

ANDERE STRAFTATEN GEGEN ÖFFENTLICHE VERWALTUNGEN

Die Begehung dieser Art von Straftaten setzt die Herstellung von Beziehungen zu öffentlichen Stellen voraus. Im Sinne des Internationalen Compliance-Programms gilt als „öffentliche Einrichtung“ in der Regel jede Einrichtung mit Rechtsstatus, die mit der Wahrung öffentlicher Interessen betraut ist und aufgrund öffentlich-rechtlichen und hoheitlichen Handlungen legislative, gerichtliche oder administrative Tätigkeiten ausübt oder die in erster Linie von staatlichen, regionalen oder lokalen Behörden oder anderen öffentlich-rechtlichen Einrichtungen finanziert wird oder deren Verwaltung und Kontrolle unterliegt.

Diese Straftaten betreffen hauptsächlich Betrug gegen öffentliche Einrichtungen und liegen vor, wenn ein Unternehmen eine oder mehrere rechtswidrige Handlungen oder Machenschaften begeht, um eine öffentliche Einrichtung zu betrügen und sich durch falsche oder betrügerische Darstellungen, Versprechungen oder Vorwände einen wirtschaftlichen Vorteil zu verschaffen.

Diese Art von Straftaten steht häufig im Zusammenhang mit öffentlichen Finanzmitteln, Subventionen und Ausschreibungen und tritt auf, wenn ein Unternehmen öffentliche Finanzmittel oder Subventionen beantragt, auf die es keinen Anspruch hat, oder diese unrechtmäßig und in einer anderen Weise als vorgesehen verwendet.



Dazu gehören auch unwahre Angaben in Bewerbungen an öffentliche Stellen, um den Zuschlag für die Ausschreibung an öffentlichen Ausschreibungsverfahren für die Vergabe einer Dienstleistung zu erhalten.

RISIKOBEREICHE

In Bezug auf diese Art von Straftaten sind folgende Risikobereiche zu überwachen:

- a) Teilnahme an Verfahren zur Vergabe öffentlicher Aufträge und Konzessionen;
- b) Durchführung von Verfahren zur Vergabe öffentlicher Aufträge und Konzessionen;
- c) Anträge auf öffentliche Mittel, Subventionen, Zuschüsse oder Bürgschaften, die von öffentlichen Stellen gewährt werden;
- d) Verwaltung öffentlicher Mittel, erhaltener Zuschüsse oder Bürgschaften;
- e) Verwaltung der Beziehungen zu Behörden (z. B. in Bezug auf Gesundheits-, Sicherheits- und Umweltauflagen, Personalverwaltung, Zahlung von Steuern).

SPEZIFISCHE VERHALTENSSTANDARDS

Die Beziehungen zu öffentlichen Stellen müssen von den Grundsätzen der Fairness, Professionalität, Loyalität und uneingeschränkter Zusammenarbeit, Ethik, Integrität, Transparenz und Einhaltung der geltenden Gesetze geprägt sein und müssen von den formell beauftragten Unternehmensstrukturen und/oder von Personen, die dazu formell befugt sind, gepflegt werden.

In Übereinstimmung mit den wichtigsten spezifischen Verhaltensstandards, die in der Antikorruptionsrichtlinie der FS Group festgelegt sind und auf die Bezug genommen werden sollte, haben ausländische Unternehmen insbesondere Folgendes zu unterlassen:

- öffentlichen Stellen Informationen oder Dokumente mit ungenauen, falschen, unvollständigen und/oder falschen Inhalten zur Verfügung zu stellen;
- die Verwendung von Geldern, Zuschüssen oder Darlehen, die von öffentlichen Stellen erhalten wurden, für andere als die vorgesehenen Zwecke;
- sich zurückhaltend oder irreführend verhalten, was die öffentliche Partei in die Irre führen könnte, auch durch das Vorenthalten von Informationen, um Entscheidungen zugunsten von Konzernunternehmen oder Dritten zu beeinflussen.

BILANZFÄLSCHUNG

Buchhaltungsbetrug ist die vorsätzliche Manipulation von Jahresabschlüssen, um ein falsches Bild der wirtschaftlichen und finanziellen Lage eines Unternehmens zu vermitteln (z. B. kann ein Unternehmen seinen Jahresabschluss fälschen, indem es Einnahmen oder Vermögenswerte überbewertet, Ausgaben nicht erfasst und Verbindlichkeiten unterbewertet).

Buchhaltungsbetrug kann aus verschiedenen Gründen zum “vermeintlichen Vorteil” des Unternehmens erfolgen, unter anderem:

- weiterhin Bankkredite aufzunehmen, obwohl die erforderlichen Voraussetzungen nicht gegeben sind;



- Angabe nicht vorhandener Gewinne oder Verschleierung von Verlusten;
- Verschleierung von Umständen, die sich nachteilig auf das Unternehmen auswirken könnten;
- Auslassen wesentlicher Fakten, die interessierte Parteien irreführen könnten;
- die Einrichtung von Schmiergeldkassen zu verschleiern.

RISIKOBEREICHE

In Bezug auf diese Art von Straftaten sind die folgenden Risikobereiche zu überwachen:

- a) Erstellung von Dokumenten, die an Aktionäre oder die Öffentlichkeit ausgegeben werden (z. B. Jahresabschlüsse, periodische Finanzberichte) und die die wirtschaftliche oder finanzielle Lage eines ausländischen Unternehmens betreffen, auch wenn diese Dokumente sich von denen unterscheiden, die für die Zwecke der periodischen Rechnungslegung erstellt werden;
- b) Verwaltung von Buchhaltungsunterlagen;
- c) Verwaltung der Geld- und Finanzströme;
- d) Verwaltung der Beziehungen zu externen Wirtschaftsprüfern.

SPEZIFISCHE VERHALTENSSTANDARDS

In Übereinstimmung mit den wichtigsten spezifischen Verhaltensstandards, die in den Verwaltungs- und Rechnungslegungsrichtlinien und -verfahren der Gruppe festgelegt sind und auf die Bezug genommen werden sollte, haben ausländische Unternehmen insbesondere Folgendes zu unterlassen:

- die Darstellung oder Übermittlung falscher, ungenauer oder unvollständiger Daten oder in jedem Fall von Daten, die nicht der tatsächlichen wirtschaftlichen, kapitalmäßigen und finanziellen Lage des Unternehmens entsprechen, bei der Erstellung und Darstellung des Unternehmens in Jahresabschlüssen, Berichten oder anderen gesetzlich vorgeschriebenen Unternehmensmitteilungen;
- das Auslassen oder Verändern relevanter Daten und Informationen über die wirtschaftliche und finanzielle Lage des Unternehmens, die in gesetzlich vorgeschriebenen Jahresabschlüssen, Berichten oder anderen Unternehmensmitteilungen verwendet werden sollen;
- Verhalten, das durch die Verschleierung von Dokumenten oder andere betrügerische Maßnahmen die Durchführung von Kontroll- oder Prüfungsmaßnahmen der Unternehmensleitung durch Aktionäre, den Rechnungsprüfungsausschuss oder ein gleichwertiges Gremium oder externe Wirtschaftsprüfer wesentlich verhindert oder in irgendeiner Weise behindert.

Jeder Vorgang oder jede Transaktion des ausländischen Unternehmens sollte gemäß den gesetzlich festgelegten Kriterien und den geltenden Rechnungslegungsstandards korrekt und unverzüglich im Rechnungslegungssystem des Unternehmens erfasst werden.

Jeder Vorgang und jede Transaktion der ausländischen Gesellschaft muss überprüfbar, rechtmäßig, konsistent und kongruent sein.



Damit die Konten den Anforderungen an Wahrhaftigkeit, Vollständigkeit und Transparenz entsprechen, müssen für jede Transaktion angemessene und vollständige Belege über die durchgeführte Tätigkeit aufbewahrt werden, um Folgendes zu ermöglichen:

- eine genaue und vollständige Darstellung der wirtschaftlichen Transaktionen des Unternehmens;
- die sofortige Ermittlung der Merkmale und Gründe der Transaktion;
- die einfache formale und chronologische Rekonstruktion der Transaktion;
- interne Kontrollen und Prüfungen durch den externen Wirtschaftsprüfer.

Jeder Buchungseintrag muss die in den Belegen enthaltenen Informationen getreu wiedergeben. Daher ist jeder Mitarbeiter dafür verantwortlich, dass die Belege leicht zugänglich und in Ordnung sind.

STEUERSTRAFTATEN

Steuerdelikte können von jeder Gerichtsbarkeit weit gefasst definiert werden, um ein breites Spektrum von Aktivitäten abzudecken, und können aus verschiedenen Gründen zum “vermeintlichen Vorteil” des Unternehmens auftreten, einschließlich, aber nicht beschränkt auf:

- Ausstellung von Dokumenten für nicht existierende Transaktionen;
- Versäumnis der Registrierung für Steuerzwecke oder Führung unrichtiger Aufzeichnungen;
- Nichtzahlung, einschließlich durch Verrechnung ungerechtfertigter Forderungen;
- Einreichung einer falschen Steuererklärung;
- Steuerhinterziehung oder Steuerrückerstattungen durch Betrug oder illegale Praktiken;
- vorsätzliche Steuerermäßigungen unter Verwendung falscher und/oder fiktiver Dokumente (einschließlich z. B. Rechnungen);
- Behinderung eines Beamten der Steuerbehörde.

RISIKOBEREICHE

In Bezug auf diese Art von Straftaten sind folgende Risikobereiche zu überwachen:

- a) Verwaltung der Unternehmensbesteuerung;
- b) Verwaltung von Buchhaltungsunterlagen und Dokumenten, die für Steuerzwecke aufzubewahren sind;
- c) Verwaltung der Erfassung, Speicherung, Aufzeichnung und Ausstellung von Rechnungen oder anderen Unterlagen, die für steuerliche Zwecke aufzubewahren sind;
- d) Erfassung und Auswertung der für die Erstellung von Jahresabschlüssen erforderlichen Buchhaltungsdaten;
- e) Verwaltung von Steuererklärungen;
- f) Verwaltung von Tätigkeiten im Zusammenhang mit der Abrechnung und Zahlung von Steuern.

SPEZIFISCHE VERHALTENSSTANDARDS

In Übereinstimmung mit der Steuerstrategie der Ferrovie dello Stato Italiane-Gruppe, auf die Bezug genommen werden sollte, sollte jedes ausländische Unternehmen:

- alle Vorschriften und ganz allgemein die geltenden Steuerbestimmungen einhalten;
- ein Verhalten an den Tag legen, das auf dem Grundsatz der äußersten Vorsicht basiert;
- sicherstellen, dass die Steuerlast gemäß den geltenden Gesetzen und den Anweisungen der Steuerbehörden korrekt ermittelt und in den Steuererklärungen angegeben wird;
- korrekte, vollständige und transparente Aufzeichnungen und Bücher führen, um sicherzustellen, dass diese die Geschäftstätigkeit des Unternehmens widerspiegeln;
- Fristen und die Einhaltung der Steuervorschriften sowie die Umsetzung neuer Steuervorschriften zu überwachen;
- regelmäßige Aktualisierungs-/Schulungsmaßnahmen für die an den Steuerfestsetzungs-/Kontrollprozessen beteiligten Personen durchführen.

ORGANISIERTE KRIMINALITÄT

Organisierte Kriminalität bezeichnet eine Form der assoziierten Kriminalität, bei der mehrere Personen zum Zweck der Begehung mehrerer Straftaten eine stabile Organisation bilden. Der Begriff „organisierte Kriminalität“ bezieht sich auch auf groß angelegte, komplexe kriminelle Aktivitäten, die von organisierten Personengruppen in undefinierter Weise oder mit komplexen Strukturen durchgeführt werden, mit dem Ziel, auf Kosten der Gemeinschaft und ihrer Mitglieder Gewinne für ihre Teilnehmer zu erzielen.

RISIKOBEREICHE

In Bezug auf diese Art von Straftaten sind folgende Risikobereiche zu überwachen:

- a) Personalauswahl, Einstellung, Management und Anreize;
- b) Auswahl von Wirtschaftsteilnehmern für die Vergabe von Bauleistungen, Dienstleistungen und Lieferungen;
- c) Verwaltung der Beziehungen zu Dritten;
- d) außerordentliche Unternehmenstransaktionen und/oder Finanzinvestitionstransaktionen und/oder Verwendung der eigenen Liquidität des Unternehmens;
- e) Investitionstätigkeiten und Joint-Venture-Vereinbarungen oder andere Formen der Partnerschaft mit lokalen oder ausländischen Partnern.

SPEZIFISCHE VERHALTENSSTANDARDS

In Bezug auf die identifizierten Risikobereiche sollte jedes ausländische Unternehmen Folgendes strikt unterlassen:

- Aufbau von Geschäftsbeziehungen oder Spenden an Dritte, wenn der begründete Verdacht besteht, dass diese Dritten Mitglieder organisierter krimineller Netzwerke sind;
- Erfüllung von Forderungen jeglicher Art, die gegen das Gesetz verstoßen, oder Zusammenarbeit mit anderen zum Zwecke der Begehung



mehrfacher Straftaten;

- sich mit Dritten zu verbünden, indem eigene, fremde oder unternehmenseigene Kenntnisse oder Mittel für eine solche Verbindung bereitgestellt werden, um Handlungen, Taten oder Operationen durchzuführen, die nicht im Einklang mit den hierin festgelegten Bestimmungen, den Unternehmensverfahren und dem Ethikkodex der Gruppe stehen oder die in jedem Fall eine Straftat darstellen können, wenn auch nur potenziell.

Darüber hinaus gilt für die Umsetzung der oben genannten Verhaltensgrundsätze:

- der Prozess der Auswahl von Wirtschaftsteilnehmern für die Vergabe von Bauleistungen, Dienstleistungen und Lieferungen muss von den Grundsätzen der Transparenz, des gleichberechtigten Zugangs, der Professionalität, der Zuverlässigkeit und der Wirtschaftlichkeit geleitet sein;
- jede Transaktion sollte über das Bankensystem abgewickelt werden, und Kunden sollten verpflichtet werden, Zahlungen ausschließlich über dieses System zu tätigen, sodass die Rückverfolgbarkeit von Finanztransaktionen ermöglicht wird;
- jeder Vorgang, einschließlich solcher außerordentlicher Art, innerhalb der Gruppe, zu der sie gehört (Umwandlungen, Fusionen, Spaltungen usw.), muss genehmigt, überprüfbar, rechtmäßig, konsistent und kongruent sein sowie ordnungsgemäß dokumentiert werden;
- Eine ständige Überwachung der Finanzströme des Unternehmens (auch im Zusammenhang mit der Verwaltung von konzerninternen Zahlungen) sollte durchgeführt werden.
- Es müssen spezifische Kontrollen der Gegenpartei festgelegt und durchgeführt werden, um deren Identität, Sitz, Rechtsform, Ruf und Zuverlässigkeit zu überprüfen, auch unter Bezugnahme auf deren Eintragung in nationalen und internationalen Referenzlisten und schwarzen Listen zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und organisierter Kriminalität.

FINANZIERUNG VON TERRORISMUS UND SOGENANNT E GELDWÄSCHEVERBRECHEN

Terrorismusfinanzierung ist definiert als die Bereitstellung oder Sammlung von Geldern – auf direktem oder indirektem Wege – mit der Absicht, diese zur Unterstützung terroristischer Handlungen oder Organisationen zu verwenden.

Für die Zwecke des internationalen Compliance-Programms kann das Phänomen der sogenannten Geldwäsche drei verschiedene Arten von Verhaltensweisen umfassen: (i) Umwandlung oder Transfer von Geldern, von denen bekannt ist, dass sie illegaler Herkunft sind;

(ii) Verschleierung oder Verdeckung der wahren Natur, Herkunft, Lage, Eigentumsverhältnisse oder anderer Rechte an Vermögenswerten, von denen bekannt ist, dass sie illegaler Herkunft sind; (iii) Erwerb, Besitz oder Verwendung von Vermögenswerten, von denen bei Erhalt bekannt ist, dass sie illegaler Herkunft sind.

Wenn die Erträge aus einer Straftat von derselben Person erzielt werden, die ihre illegale Herkunft verschleiert, wird ein solches Verhalten in einigen Ländern als Selbstgeldwäsche bestraft. Geldwäsche und Terrorismusfinanzierung weisen oft ähnliche Transaktionsmerkmale auf, die meist mit der Verschleierung zusammenhängen.



Diejenigen, die Geldwäsche betreiben, transferieren illegale Gelder über legale Kanäle, um deren kriminelle Herkunft zu verschleiern, während diejenigen, die Terrorismus finanzieren, Gelder legaler oder illegaler Herkunft so transferieren, dass deren Herkunft und letztendliche Verwendung, d. h. die Unterstützung des Terrorismus, verschleiert wird.

Diese Art von Verhalten kann zum “vermeintlichen Vorteil” eines Unternehmens erfolgen, einschließlich, aber nicht beschränkt auf:

- Erträge oder sonstige Vorteile aus illegalen Aktivitäten der finanzierten terroristischen Organisationen zu erzielen (andere Vorteile können im Schutz von Geschäften in Ländern bestehen, in denen diese Organisationen einen erheblichen Einfluss haben);
- die illegale Herkunft der Erträge aus Straftaten zu verschleiern.

RISIKOBEREICHE

In Bezug auf diese Art von Straftaten sind folgende Risikobereiche zu überwachen:

- a) Vertragsbeziehungen mit Wirtschaftsteilnehmern, die mit Bauleistungen, Dienstleistungen und Lieferungen betraut sind, Partnern und anderen juristischen Personen, die direkt oder indirekt von den oben genannten Einrichtungen kontrolliert werden und ihren Wohnsitz oder Sitz in einem Land haben, das eine risikoreiche und nicht kooperative Gerichtsbarkeit darstellt;
- b) Verwaltung von Geld- und Finanzströmen.

SPEZIFISCHE VERHALTENSSTANDARDS

Um jegliches Verhalten zu vermeiden, das auch nur indirekt darauf abzielt, Straftaten wie Hehlerei, Geldwäsche und die Verwendung von Geld, Gütern oder anderen Vermögenswerten illegaler Herkunft, die Finanzierung von Terrorismus sowie jegliche missbräuchliche Verwendung von Finanzinstrumenten und/oder Transaktionen zur Verschleierung der Herkunft der Unternehmensmittel zu erleichtern, sollte jedes ausländische Unternehmen:

- das Bankensystem für die Durchführung von Transaktionen nutzen und von Kunden verlangen, Zahlungen ausschließlich über dieses System zu tätigen, das die Rückverfolgbarkeit von Finanzbewegungen ermöglicht, wobei keine Zahlungen „außerhalb der Bücher“, d. h. auf Konten in anderen Ländern als dem des eingetragenen Firmensitzes/Wohnsitzes oder in den im Vertrag angegebenen Ländern, vorgeschlagen oder akzeptiert werden dürfen;
- Unternehmens-Kreditkarten, Prepaid-Karten und/oder andere Zahlungsinstrumente angemessen und in Übereinstimmung mit den Unternehmenszielen zu verwenden und dabei auf die Sicherung und den Schutz der relevanten Daten zu achten;
- alle Daten über Geschäftspartner auf dem neuesten Stand zu halten, um eine valide Bewertung ihrer Geschäftsprofile zu ermöglichen;
- keine Geschäfte mit natürlichen oder juristischen Personen tätigen, von denen bekannt ist oder vermutet wird, dass sie kriminellen oder anderweitig illegalen Organisationen angehören;
- sicherstellen, dass jede Transaktion, auch wenn sie außergewöhnlicher Natur ist, innerhalb der betreffenden Gruppe (Umwandlungen, Fusionen, Spaltungen usw.) genehmigt, überprüfbar, rechtmäßig, konsistent und kongruent ist sowie ordnungsgemäß



aufgezeichnet wird;

- die Vorschriften für eine korrekte, vollständige und transparente Erfassung der Buchungen im Zusammenhang mit der Unternehmensführung einhalten;
- die Cashflows entsprechend den verschiedenen Aktivitäten, die im Rahmen der Geschäftstätigkeit des Unternehmens durchgeführt werden, ständig überwachen;
- das für die die Kreditkartenverwaltung zuständige Personal identifizieren, und die Kriterien für die Zuteilung von Firmenkreditkarten und der Verfahren für deren Verwendung einhalten;
- spezifische Kontrollen einführen und umsetzen, die bei der Gegenpartei durchzuführen sind, um deren Identität, Sitz, Rechtsform, Ruf und Zuverlässigkeit zu überprüfen, auch hinsichtlich ihrer Präsenz in nationalen und internationalen Referenzlisten und schwarzen Listen zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und organisierter Kriminalität.

MARKTMISSBRAUCH

Marktmissbrauch kann sich auf verschiedene Verhaltensweisen beziehen, wie z. B.:

- Besitz von Insiderinformationen, um Transaktionen (Käufe, Verkäufe usw.) mit Finanzinstrumenten durchzuführen oder andere dazu zu veranlassen;
- Weitergabe solcher Insiderinformationen an andere;
- Verbreitung falscher Informationen, um eine erhebliche Veränderung des Kurses von Finanzinstrumenten zu bewirken;
- Durchführung von Scheingeschäften oder anderen Maßnahmen, um eine erhebliche Veränderung des Preises von Finanzinstrumenten zu bewirken.

Ein solches Verhalten kann aus verschiedenen Gründen zum “vermeintlichen Vorteil” eines Unternehmens erfolgen, darunter unter anderem:

- Senkung des Kurses der Finanzinstrumente eines Zielunternehmens vor einer Übernahme;
- die Schwächung des Rufs eines Konkurrenzunternehmens;
- Veränderung des Kurses eines bestimmten Finanzinstruments im Portfolio, bevor Handelsaktivitäten in Bezug auf dieses Instrument durchgeführt werden.

RISIKOBEREICHE

In Bezug auf diese Art von Straftaten sind folgende Risikobereiche zu überwachen:

- a) Verwaltung von Informationen, die der Öffentlichkeit zugänglich gemacht werden (Beziehungen zu Investoren, Finanzanalysten, Ratingagenturen, Journalisten und anderen Vertretern der Massenmedien, einschließlich der Verwaltung von Werbekampagnen; Organisation von und Teilnahme an Treffen jeglicher Art mit den oben genannten Parteien);
- b) Verwaltung von Insiderinformationen, die die Wertentwicklung börsennotierter Finanzinstrumente beeinflussen können



(z. B. Informationen, die in engem Zusammenhang mit neuen Dienstleistungen und Märkten stehen, Rechnungslegungsdaten für den Berichtszeitraum, Prognosedaten und quantitative Ziele in Bezug auf die Geschäftsentwicklung, Mitteilungen über Fusionen/Spaltungen und neue Initiativen von besonderer Bedeutung oder Verhandlungen und/oder Vereinbarungen über den Erwerb und/oder die Veräußerung bedeutender Vermögenswerte, M&A-Aktivitäten);

- c) Erstellung von Rechnungslegungsunterlagen und Prospekten, die aufgrund gesetzlicher Vorschriften oder aufgrund von Unternehmensentscheidungen zu veröffentlichen sind;
- d) jede Art von Transaktion im Zusammenhang mit den Finanzinstrumenten im Portfolio.

SPEZIFISCHE VERHALTENSSTANDARDS

In Übereinstimmung mit den Regulierungsinstrumenten der Gruppe zum Marktmissbrauch, auf die Bezug genommen wird, ist jedes ausländische Unternehmen ausdrücklich verpflichtet, Folgendes zu unterlassen:

- die Weitergabe von vertraulichen Informationen an Dritte, außer in Fällen, in denen eine solche Weitergabe aufgrund von Gesetzen oder Vorschriften, durch Justiz- oder Verwaltungsbehörden, durch Bestimmungen oder durch spezifische vertragliche Vereinbarungen erforderlich ist, wenn diese Informationen darauf abzielen, das ausländische Unternehmen zu begünstigen oder ihm anderweitig einen Vorteil zu verschaffen;
- Dritten zu empfehlen oder sie dazu zu veranlassen, auf der Grundlage von Insiderinformationen (die von Unternehmensvertretern aufgrund ihrer Position innerhalb der Gruppe oder von Dritten aufgrund ihrer Geschäftsbeziehungen mit der Gruppe erhalten wurden) Käufe, Verkäufe oder andere Transaktionen mit Finanzinstrumenten zu tätigen, wenn die Durchführung solcher Transaktionen darauf abzielt, das ausländische Unternehmen zu begünstigen oder ihm in irgendeiner Weise einen Vorteil zu verschaffen;
- die Übermittlung oder Verbreitung falscher oder irreführender Insiderdaten oder Informationen über Finanzinstrumente oder Nachrichten, deren Wahrheitsgehalt nicht sicher ist und die den Wert eines Finanzinstruments verändern könnten, über beliebige Kommunikationskanäle;
- Durchführung von Transaktionen, die falsche Signale über den Wert eines Finanzinstruments senden können, um andere Händler zu Handlungen zu veranlassen, die weitere Preisänderungen hervorrufen können.

STRAFTATEN GEGEN PERSONEN

Verbrechen gegen Personen können begangen werden, indem Arbeitnehmer unter ausbeuterischen Bedingungen angeworben, eingestellt und beschäftigt werden und ihre Notlage ausgenutzt wird. Darüber hinaus können Verbrechen gegen Personen alle Handlungen umfassen, die die Achtung der Menschen und der Menschenrechte in all ihren Formen verletzen, einschließlich ethnischer, kultureller, religiöser, herkunftsbezogener und geschlechtsspezifischer Unterschiede. Das Vorliegen einer oder mehrerer der folgenden Bedingungen kann ein Hinweis auf Ausbeutung zum “vermeintlichen Vorteil” des Unternehmens sein:



- wiederholte Vergütung in einer Weise, die offensichtlich von den gesetzlichen Bestimmungen abweicht oder in jedem Fall in keinem Verhältnis zur Quantität und Qualität der geleisteten Arbeit steht;
- wiederholte Verstöße gegen Gesetze zu Arbeitszeiten, Pausen, Feiertagen und Pflichturlaub;
- Verstöße gegen Arbeitsschutzvorschriften;
- Unterwerfung der Arbeitnehmer unter menschenunwürdige Arbeitsbedingungen, Überwachungsmethoden oder Wohnverhältnisse.

RISIKOBEREICHE

In Bezug auf diese Art von Straftaten gelten folgende Risikobereiche:

- a) Auswahl, Einstellung und Verwaltung von Personal, insbesondere im Hinblick auf die Festlegung von Arbeitszeiten, Vergütung, Auswirkungen auf Gesundheit und Sicherheit sowie Arbeitsbedingungen im Allgemeinen;
- b) Zuweisung von Tätigkeiten, die den Einsatz von Arbeitskräften Dritter für die Erbringung von Arbeitsleistungen und/oder Dienstleistungen beinhalten, auch in Bezug auf Wirtschaftsteilnehmer, die in Ländern tätig sind, in denen die Rechte des Einzelnen durch internationales oder lokales Recht nicht vollständig geschützt sind.

SPEZIFISCHE VERHALTENSSTANDARDS

Ausländische Unternehmen sind verpflichtet, die folgenden Grundsätze einzuhalten:

- bei der direkten Einstellung von Personal die Einhaltung des Arbeitsrechts in Bezug auf den Einstellungsprozess und das Arbeitsverhältnis im Allgemeinen zu überprüfen;
- von Wirtschaftsteilnehmern, die Arbeits-, Dienstleistungs- und Lieferverträge vergeben, und deren Subunternehmern die Einhaltung aller geltenden internationalen und lokalen Rechtsvorschriften in Bezug auf Zwangsarbeit, den Schutz von Kindern und Frauen am Arbeitsplatz sowie hygienische Bedingungen zu verlangen;
- Einführung und Umsetzung spezifischer Kontrollen der Gegenpartei, um deren Ruf und Zuverlässigkeit zu überprüfen;
- die moralische und persönliche Integrität von Personen zu schützen, indem Arbeitsbedingungen geschaffen werden, die die Würde des Einzelnen achten und ein sicheres und gesundes Arbeitsumfeld gewährleisten;
- Gewährleistung der uneingeschränkten Achtung der Menschen und der Menschenrechte in all ihren Formen, einschließlich der Achtung ethnischer, kultureller, herkunftsbezogener und religiöser Unterschiede.

STRAFTATEN GEGEN GESUNDHEIT UND SICHERHEIT

Verstöße gegen Gesundheits- und Sicherheitsvorschriften betreffen in erster Linie die Nichteinhaltung lokaler Gesetze und Arbeitsplatzstandards, die zur Verhütung von Unfällen und Erkrankungen am Arbeitsplatz dienen, einschließlich tödlicher Unfälle oder solcher, die zu schweren oder sehr schweren Verletzungen von Mitarbeitern führen und gegen Arbeitsschutzvorschriften verstoßen.



Ein solches Verhalten kann aus einer Reihe von Gründen zum “vermeintlichen Vorteil” eines Unternehmens erfolgen, darunter unter anderem:

- eine Kostensenkung durch die Nichtumsetzung der erforderlichen Sicherheitsmaßnahmen zur Gewährleistung der Gesundheit und Sicherheit am Arbeitsplatz;
- eine Steigerung der Produktivität, da die Ausführung von Arbeitsaufgaben ohne Berücksichtigung von Vorsichtsmaßnahmen und Richtlinien die Arbeitsprozesse beschleunigen könnte.

RISIKOBEREICHE

In Bezug auf diese Art von Straftaten sollten die folgenden Bereiche als risikobehaftet angesehen werden:

a) Einhaltung der geltenden Gesundheits- und Sicherheitsvorschriften.

SPEZIFISCHE VERHALTENSSTANDARDS

Alle ausländischen Unternehmen müssen geeignete Arbeitsschutzmanagementsysteme einführen. Ziel ist es, Risiken zu kontrollieren, die Sicherheit der Beschäftigten in allen Arbeitsphasen zu gewährleisten und notwendige Maßnahmen zum Schutz von Arbeitnehmern, Dritten und den betroffenen Gemeinden zu ergreifen. Zudem ist eine wirksame Arbeitsschutzkultur zu fördern, die das Bewusstsein für Risiken und die persönliche Verantwortung stärkt.

Insbesondere sollte das von ausländischen Unternehmen eingeführte und wirksam umgesetzte Arbeitsschutzmanagementsystem:

- die Einhaltung der gesetzlichen Bestimmungen über die Gesundheit und Sicherheit der Arbeitnehmer am Arbeitsplatz als Priorität betrachten;
- die Risiken für die Gesundheit und Sicherheit der Arbeitnehmer an der Quelle beseitigen und, wo dies nicht möglich ist, sie durch erworbenes Wissen und technologischen Fortschritt auf ein Minimum reduzieren;
- ständig spezifische Risikobewertungsmaßnahmen durchführen, auch um die Einführung entsprechender Präventions- und Schutzmaßnahmen zu bewerten;
- im Falle von Konzessionen oder von Unteraufträgen für Arbeiten, Dienstleistungen oder Lieferungen durch das Unternehmen die Auftragnehmer über die Risiken informieren, die in den Arbeitsumgebungen, in denen sie tätig sein werden, bestehen;
- jeden Arbeitsunfall überwachen und analysieren, um etwaige Mängel im Gesundheits- und Sicherheitsmanagementsystem zu ermitteln und gegebenenfalls zu ergreifende Korrekturmaßnahmen festzulegen;
- regelmäßige Informations- und Schulungsmaßnahmen für die Mitarbeiter durchführen;
- Kontrollen durchführen, um die Anwendung und Wirksamkeit der Arbeitssicherheitsverfahren und -anweisungen durch Arbeitnehmer und Auftragnehmer sicherzustellen.



Um eine angemessene Überwachung der Risikobereiche sicherzustellen, muss jedes ausländische Unternehmen organisatorische, technische und finanzielle Ressourcen bereitstellen. Dadurch wird sowohl die vollständige Einhaltung der geltenden Vorschriften zur Verhütung von Arbeitsunfällen gewährleistet als auch die kontinuierliche Verbesserung von Gesundheits- und Sicherheitsbedingungen am Arbeitsplatz – unter anderem durch die Umsetzung und regelmäßige Aktualisierung geeigneter Präventionsmaßnahmen.

UMWELTKRIMINALITÄT

Umweltkriminalität umfasst rechtswidrige Handlungen, die Schäden an der Umwelt verursachen. Diese Straftaten beziehen sich auf eine Vielzahl illegaler Aktivitäten, wie beispielsweise Straftaten gegen wildlebende Tiere, den illegalen Handel und die illegale Entsorgung gefährlicher Stoffe sowie viele andere Verhaltensweisen, die der Umwelt schaden können.

Beispielsweise könnten solche Straftaten bei folgenden Aktivitäten begangen werden:

- Verwaltung von Abfallsammlung, -lagerung, -transport und -entsorgung, auch durch Auslagerung der Tätigkeiten an Dritte;
- Verwaltung von Emissionen aus industriellen Aktivitäten;
- Betrieb und Wartung von Anlagen/Geräten, die umweltschädliche Stoffe verwenden.

Umweltverbrechen können aus verschiedenen Gründen im “vermeintlichen Interesse” eines Unternehmens begangen werden, darunter:

- um die Kosten zu senken, die entstehen, wenn die notwendigen Maßnahmen zum Schutz der Umwelt nicht ergriffen werden;
- um die Produktivität zu steigern, da eine Geschäftstätigkeit ohne Berücksichtigung von Umweltaspekten den Produktionsprozess beschleunigen könnte.

RISIKOBEREICHE

In Bezug auf diese Art von Straftaten sollten die folgenden Bereiche überwacht werden, da sie als gefährdet gelten:

- a) Einhaltung der geltenden Umweltgesetze, einschließlich während der Planung, des Baus, des Betriebs und der Instandhaltung von Infrastruktur;
- b) Auswahl von Dritten zur Durchführung bestimmter Tätigkeiten, die Auswirkungen auf die Umwelt haben können (z. B. Abfallwirtschaft und -entsorgung).

SPEZIFISCHE VERHALTENSSTANDARDS

Alle ausländischen Unternehmen sollten im Rahmen ihrer Aktivitäten der Achtung und dem Schutz der Umwelt Vorrang einräumen, insbesondere durch:

- die Bewertung potenzieller Risiken und die Entwicklung geeigneter Präventionsprogramme zum Schutz der Umwelt und der öffentlichen Sicherheit;
- die Einrichtung spezifischer Verfahren in Übereinstimmung mit den geltenden Umweltgesetzen;
- die Verbreitung von Informationen zum Umweltschutz innerhalb des Unternehmens, die Förderung des Bewusstseins



und die Sicherstellung, dass die Aktivitäten in Übereinstimmung mit den geltenden Gesetzen durchgeführt werden;

- die Einführung geeigneter Maßnahmen, um zu verhindern, dass ihre Aktivitäten in irgendeiner Form Schäden und Beeinträchtigungen für das Ökosystem verursachen.

COMPUTERKRIMINALITÄT

Computerkriminalität umfasst ein breites Spektrum von Aktivitäten, die alle Bereiche des Unternehmens betreffen. Im Allgemeinen lassen sich diese Straftaten in zwei Kategorien einteilen: (i) Straftaten, die auf ein Computernetzwerk oder ein Computergerät abzielen; (ii) Straftaten, die durch die Nutzung von Computernetzwerken oder Computergeräten erleichtert werden.

Die in diesem Dokument behandelten Computerkriminalitätsdelikte umfassen beispielsweise: (i) das unbefugte Eindringen in ein geschütztes Computernetzwerk; (ii) das Einschleusen von Viren in ein Computersystem; (iii) das Abfangen von Daten aus einem Computernetzwerk; (iv) die Störung eines Computersystems durch Beschädigung, Löschung, Veränderung oder Unterdrückung von Computerdaten; (v) die rechtswidrige Beeinträchtigung des Betriebs eines Computersystems; (vi) Computerbetrug und betrügerische Verwendung von Computerdaten, um sich einen ungerechtfertigten finanziellen Vorteil zu verschaffen.

Computerkriminalität kann aus verschiedenen Gründen im “vermeintlichen Interesse” eines Unternehmens begangen werden, darunter:

- um Zugang zu den Geschäftsgeheimnissen eines Konkurrenzunternehmens zu erhalten;
- um vertrauliche Informationen über die Marktstrategien konkurrierender Unternehmen zu erhalten;
- um das Computersystem eines Konkurrenzunternehmens zu gefährden oder zu beschädigen;
- um kritische Computersysteme eines Konkurrenten, beispielsweise solche, die mit der wesentlichen Infrastruktur oder Produktion in Zusammenhang stehen, zu kompromittieren und so erheblichen Schaden anzurichten.

RISIKOBEREICHE

In Bezug auf diese Art von Straftaten sollten die folgenden Bereiche als Risikobereiche betrachtet werden:

- a) Geschäftstätigkeiten, die unter Verwendung von IT-Tools (z. B. dem E-Mail-System) durchgeführt werden;
- b) Verwaltung und Schutz von Arbeitsplätzen, Laptops, Mobiltelefonen und Speichergeräten;
- c) Festlegung der physischen und logischen Sicherheitsmaßnahmen, die für das Computersystem zu treffen sind, einschließlich der Klassifizierung und Verarbeitung von Informationen und Daten sowie der Verwaltung von Systemadministratorprofilen;
- d) Maßnahmen zur Sicherung von Unternehmensnetzwerken, einschließlich der Verschlüsselung der Kommunikation und der Abwehr von Netzwerkangriffen, die für die Verhinderung von unbefugtem Zugriff und Datenkompromittierung unerlässlich sind.



SPEZIFISCHE VERHALTENSSTANDARDS

Als allgemeiner Präventionsgrundsatz, der für alle Geschäftsprozesse gilt, bei denen das Risiko von Computerkriminalität besteht, müssen alle ausländischen Unternehmen sicherstellen, dass der Zugriff auf und die Verarbeitung von Daten in Computersystemen in Übereinstimmung mit den geltenden gesetzlichen Bestimmungen erfolgt.

Ausländische Unternehmen müssen gemäß den geltenden lokalen Gesetzen eine regelmäßige Überwachung der Aktivitäten ihrer Mitarbeiter im Computersystem des Unternehmens sicherstellen, um ungewöhnliches Verhalten und potenzielle Schwachstellen in den Systemen des Unternehmens aufzudecken.

Darüber hinaus müssen ausländische Unternehmen Sensibilisierungskampagnen durchführen, gegebenenfalls auch durch spezifische Schulungen, um auf die Bedeutung einer korrekten und angemessenen Nutzung der im Rahmen der Unternehmensaktivitäten eingesetzten IT-Tools hinzuweisen.

In Bezug auf die Nutzung und Verwaltung von Computersystemen, Tools, Dokumenten oder Daten müssen ausländische Unternehmen die folgenden Kontrollgrundsätze einhalten:

- Einhaltung der Verfahren zum IT-Sicherheitsmanagement;
- Erstellung und Umsetzung einer Unternehmensrichtlinie für die Verwaltung und Überwachung der physischen Sicherheit von IT-Umgebungen und -Ressourcen;
- Einführung spezifischer Maßnahmen zur Gewährleistung der Aufgabentrennung im Änderungsmanagementprozess (Neuentwicklungen, evolutionäre Wartung, korrektive Wartung und routinemäßige Wartung) von IT-Systemen (Anwendungs- oder Basissoftware, Hardware und Systeme);
- Bereitstellung und Umsetzung von Notfallwiederherstellungsprozessen und -mechanismen, um die Wiederherstellung bestimmter Systeme und Daten im Falle einer vorübergehenden Nichtverfügbarkeit oder eines dauerhaften Verlusts sicherzustellen;
- Ergreifen spezifischer Maßnahmen, um sicherzustellen, dass die Nutzung von Vermögenswerten, die möglicherweise durch Rechte des geistigen Eigentums geschützt sind, den gesetzlichen oder vertraglichen Bestimmungen entspricht;
- Implementierung eines Schutzsystems, das geeignet ist, zuvor autorisierte Benutzer, die auf ein Verarbeitungs- oder Übertragungssystem zugreifen, zu identifizieren und zu authentifizieren;
- Bereitstellung technologischer Tools und Schutzstufen gegen Spam, Spyware, Malware usw.;
- Aktivierung geeigneter Filter, um den Zugriff auf Websites zu verhindern, die für die Arbeit nicht relevant oder verboten sind;
- Entzug der Berechtigung zur Nutzung eines Computersystems/einer Anwendung bei Beendigung des Arbeitsverhältnisses, Wechsel der Position im Unternehmen oder als Folge längerer Nichtnutzung;
- Implementierung fortschrittlicher Lösungen zur Überwachung des Netzwerkverkehrs und der Benutzeraktivitäten auf Computersystemen, einschließlich der Verwendung von Anomalieerkennungssystemen und detaillierten Benutzeraktivitätsprotokollen, um ungewöhnliches Verhalten, verdächtige Aktivitäten oder unbefugten Zugriff zu erkennen;



- Durchführung regelmäßiger IT-Sicherheitsaudits, um die Wirksamkeit der implementierten Sicherheitsmaßnahmen zu bewerten, potenzielle Schwachstellen zu identifizieren und kontinuierliche Verbesserungen vorzunehmen;
- Durchführung regelmäßiger Sicherheitstests und simulierter Angriffe, um die Bereitschaft der Organisation zu bewerten, Schwachstellen zu identifizieren und die Reaktion auf Vorfälle zu verbessern.

URheberRECHTSVERLETZUNGEN

Eine Urheberrechtsverletzung kann in der unbefugten Nutzung von Werken bestehen, die durch das Urheberrecht und das Recht des geistigen/gewerblichen Eigentums geschützt sind, d. h. unter Verletzung bestimmter ausschließlicher Rechte, die dem Inhaber des Urheberrechts und/oder des Rechts des geistigen/gewerblichen Eigentums zustehen, wie z. B. das Recht, das geschützte Werk zu vervielfältigen, zu verbreiten, auszustellen oder aufzuführen oder davon abgeleitete Werke zu erstellen.

RISIKOBEREICHE

In Bezug auf diese Art von Straftaten sind folgende Risikobereiche zu überwachen:

- a) die Installation, der Betrieb, die Nutzung und die Vervielfältigung von urheberrechtlich und/oder durch geistige/gewerbliche Schutzrechte geschützter Software innerhalb der Computersysteme des Unternehmens;
- b) Verwendung von Texten, Bildern, Musik und Videos, die durch Urheberrecht und/oder geistiges/gewerbliches Eigentumsrecht geschützt sind, innerhalb der Computersysteme des Unternehmens;
- c) Verwaltung von geistigen und gewerblichen Eigentumsrechten in Bezug auf Marken, Patente, Erfindungen, Designs und Gebrauchsmuster.

SPEZIFISCHE VERHALTENSSTANDARDS

Ausländische Unternehmen ergreifen geeignete technische, physische und organisatorische Maßnahmen, um Folgendes zu vermeiden:

- jede rechtswidrige Nutzung oder Verbreitung an die Öffentlichkeit, einschließlich über Computernetzwerke oder Verbindungen anderer Art, des durch das Urheberrecht und/oder das Recht des geistigen/gewerblichen Eigentums geschützten Originalwerks oder eines Teils davon;
- die Nutzung von Vermögenswerten, die durch erworbene Rechte geschützt sind, für geschäftliche Zwecke unter Umgehung der durch das Urheberrecht und/oder das Recht des geistigen/gewerblichen Eigentums auferlegten Verpflichtungen oder in einer Weise, die vom Eigentümer nicht beabsichtigt ist;
- das illegale Herunterladen von Software ohne entsprechende vertragliche Unterlagen.

Wenn ein ausländisches Unternehmen einen Vertrag mit externen Auftragnehmern über die Durchführung von Tätigkeiten abschließt, die potenziell als Verstoß gegen Urheberrechte/Eigentumsrechte angesehen werden könnten, muss dieser Vertrag außerdem Klauseln enthalten, die den Auftragnehmer zur Einhaltung der geltenden Gesetze und Vorschriften zu diesem Thema verpflichten.

SCHMUGGEL

Schmuggel liegt vor, wenn eine natürliche oder juristische Person Waren ausländischer Herkunft entfernt oder zu verstecken versucht, um die Zahlung der entsprechenden Grenzabgaben zu umgehen. Im Allgemeinen besteht Schmuggel in der illegalen Ein- oder Ausfuhr von Waren unter Verstoß gegen die Zollbestimmungen und Gesetze eines Staates, die deren Einfuhr, Ausfuhr und Beförderung verbieten oder besteuern.

RISIKOBEREICHE

In Bezug auf diese Art von Straftaten sind die folgenden Risikobereiche zu überwachen:

- a) Zollkonformitätsmanagement (Erstellung und Übermittlung gesetzlich vorgeschriebener Unterlagen, Pflege der Beziehungen zu den Zollbehörden, auch mit Unterstützung Dritter usw.);
- b) Zahlung von Zöllen und Übermittlung von Dokumenten im Zusammenhang mit der Ein- und Ausfuhr von Materialien an die Zollbehörden;
- c) Auswahl der Wirtschaftsbeteiligten, die Waren liefern, sowie Verhandlung, Abschluss und Verwaltung der entsprechenden Verträge;
- d) Lagerverwaltung.

SPEZIFISCHE VERHALTENSSTANDARDS

Zusätzlich zu den Bestimmungen der Sanktionsrichtlinie der FS-Gruppe, auf die verwiesen wird, müssen ausländische Unternehmen:

- sicherstellen, dass alle Aktivitäten und Vorgänge unter strikter Einhaltung der einschlägigen Vorschriften durchgeführt werden;
- Festlegung von Betriebsverfahren für die direkte oder indirekte Durchführung von Zollvorgängen und die damit verbundene Überwachung.

VERBRECHEN GEGEN DAS KULTURELLE ERBE

Verbrechen gegen das Kulturerbe umfassen alle Straftaten, die das Kulturerbe als kollektives Rechtsgut oder Gemeingut betreffen, das nicht nur aus rein privater materieller Sicht geschützt ist, sondern vor allem auch als Wert an sich, da es eine öffentliche Komponente darstellt, die ein Instrument der Kultur ist, das der intellektuellen Bildung aller Menschen dient.

Beispielsweise können folgende Straftaten in die Kategorie der Straftaten gegen das kulturelle Erbe fallen:

- Verbreitung (z. B. Diebstahl und Veruntreuung von Kulturgütern);
- illegaler Handel (z. B. Verstöße im Zusammenhang mit der Veräußerung, der illegalen Ein- und Ausfuhr von Kulturgütern);



- Fälschung (Fälschung privater Dokumente im Zusammenhang mit Kulturgütern und Fälschung von Kunstwerken);
- Verschleierung der illegalen Herkunft (Hehlerei und Geldwäsche von Kulturgütern);
- Zerstörung (Zerstörung, Zerstreuung, Beschädigung, Verunstaltung und rechtswidrige Nutzung von Kulturgütern oder Umweltgütern, Verwüstung und Plünderung von Kulturgütern oder Umweltgütern).

RISIKOBEREICHE

In Bezug auf diese Art von Straftaten sind folgende Risikobereiche zu überwachen:

- a) Verwaltung des beweglichen und unbeweglichen Kulturerbes.

SPEZIFISCHE VERHALTENSSTANDARDS

Alle ausländischen Unternehmen müssen:

- die Vorschriften zum Schutz des kulturellen und ökologischen Erbes einhalten, insbesondere durch die Einführung aller geeigneten Kontrollen und Maßnahmen zum Schutz des Erbes selbst;
- zur Erfüllung aller gesetzlichen Verpflichtungen beitragen, einschließlich derjenigen, die sich auf den Erwerb und den Verkehr von Kulturgütern beziehen oder anderweitig zum Schutz des kulturellen und ökologischen Erbes erforderlich sind;
- die Erwerbsphasen von Kulturgütern überwachen, einschließlich der Überprüfung ihrer Herkunft (z. B. durch Einholung nützlicher und notwendiger Bescheinigungen und Genehmigungen vom Verkäufer/Lieferanten).