Verfahren von ArcelorMittal zum Datenschutz
Endgültige Version

Die Bearbeitung personenbezogener Daten ist in vielen Ländern, in denen ArcelorMittal tätig ist, gesetzlich geregelt. ArcelorMittal erkennt an, dass personenbezogene Daten mit Sorgfalt zu behandeln sind, unabhängig davon, ob es sich um die Daten von Mitarbeitern oder von Geschäftspartnern handelt. Daher möchte ArcelorMittal praktische und rechtliche Maßnahmen zum Schutz personenbezogener Daten ergreifen, die unter der Verantwortung der Gesellschaft verarbeitet werden.

Ziel dieses Verfahrens ist es, einheitliche, angemessene und globale Datenschutzstandards aufzustellen und die konzernweite Übermittlung personenbezogener Daten gemäß den Anforderungen der Datenschutzgesetze zu ermöglichen.

Definitionen

Definitionen

Tochtergesellschaft
"Tochtergesellschaft" ist eine Gesellschaft oder Wirtschaftseinheit, die von ArcelorMittal SA, eingetragen im Gesellschafts- und Handelsregister von Luxemburg unter Nr. B 82 454, vollkonsolidiert und kontrolliert wird.
Unter dem Begriff "Kontrolle" ist dabei der direkte oder, durch einen oder mehrere Vermittler, indirekte Besitz der Macht zu verstehen, die Geschäftsführung und die Richtlinien einer Gesellschaft oder Wirtschaftseinheit durch den Besitz stimmberechtigter Anteile, im Wege von Verträgen oder auf sonstige Weise zu steuern oder steuern zu lassen.

Personenbezogene Daten
"Personenbezogene Daten" sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Betroffener
"Betroffener" ist eine natürliche Person, deren personenbezogene Daten von einer Tochtergesellschaft im Zusammenhang mit einem unter den Anwendungsbereich dieses Verfahrens fallenden Prozess verarbeitet werden.

Verarbeitung
"Verarbeitung" personenbezogener Daten ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Wiederauffinden, das Abfragen, die Nutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten;

Besondere Kategorien von Daten ("Besondere Daten")
"Besondere Daten" sind personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit und Daten über Gesundheit oder Sexualleben hervorgehen.

Personaldaten
"Personaldaten" sind personenbezogene Daten von Mitarbeitern, Bewerbern, Trainees, Zeitarbeitskräften oder ehemaligen Mitarbeitern der ArcelorMittal Tochtergesellschaften.

Globale Tools/Datenbanken

"Globale Tools/Datenbanken" sind IT Tools (i), die personenbezogene Daten enthalten und (ii) nicht auf einen Standort, einen Unternehmensbereich, ein Segment beschränkt sind.
Beispiel:
One HRIS

Herr der Daten
"Herr der Daten" ist die natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

Auftragsverarbeiter
"Auftragsverarbeiter" ist eine juristische Person, die personenbezogene Daten im Auftrag des Herrn der Daten verarbeitet. Das Wort "Auftragsverarbeiter" hat die gleiche Bedeutung wie der Begriff "Anbieter", der üblicherweise bei ArcelorMittal verwendet wird.

ArcelorMittal Auftragsverarbeiter
"ArcelorMittal Auftragsverarbeiter" ist ein Auftragsverarbeiter, der eine ArcelorMittal Tochtergesellschaft ist.

Europa ("EU")
Europa bezeichnet die 27 Mitgliedsstaaten der Europäischen Union per November 2010 + die 3 Mitglieder des EWR:
Island
Liechtenstein
Norwegen
Österreich
Belgien
Bulgarien
Zypern
Tschechische Republik
Dänemark
Estland
Finnland
Frankreich
Deutschland
Griechenland
Ungarn
Irland
Italien
Lettland
Litauen
Luxemburg
Malta
Niederlande
Polen
Portugal
Rumänien
Slowakei

Slowenien
Spanien
Schweden
Vereinigtes Königreich

Datenexporteur
"Datenexporteur" ist eine in Europa ansässige Tochtergesellschaft, die personenbezogene Daten in Europa verarbeitet, die dann an eine Tochtergesellschaft außerhalb Europas weitergeleitet oder dieser zugänglich gemacht werden.

Datenimporteur
"Datenimporteur" ist eine außerhalb Europas ansässige Tochtergesellschaft, die personenbezogene Daten verarbeitet, die dann an eine in Europa ansässige Tochtergesellschaft übermittelt oder dieser zugänglich gemacht werden.

Die Bedingungen dieses Verfahrens sind gemäß den Richtlinien (EU) 95/46/EG und 2002/58/EG auszulegen.

Artikel 1 - Status des Verfahrens

Die Konzernleitung / *Group Management Board* von ArcelorMittal trägt die Gesamtverantwortung für die Umsetzung dieses Verfahrens.

Alle Verwaltungsratsmitglieder, Führungskräfte und Mitarbeiter von ArcelorMittal und seinen Tochtergesellschaften weltweit, die personenbezogene Daten verarbeiten, haben dieses Verfahren einzuhalten.

Jeder, der gegen dieses Verfahren verstößt, wird gemäß den jeweils anwendbaren lokalen Gesetzen und Richtlinien Disziplinarmaßnahmen unterzogen.

ArcelorMittal erkennt an, dass einige Gesetzt strengere als die in diesem Verfahren beschriebenen Standards vorsehen. In diesem Fall werden die Tochtergesellschaften von ArcelorMittal personenbezogene Daten gemäß den jeweils am Ort der Verarbeitung der personenbezogenen Daten geltenden Gesetzen verarbeiten. Sollten die zur Anwendung kommenden lokalen Gesetze einen geringeren Schutz personenbezogener Daten vorsehen als dieses Verfahren, gelten die Anforderungen dieses Verfahrens.

Zur Regelung der Nutzung bestimmter Tools/Datenbank wurden und werden spezifische Datenschutzbestimmungen entwickelt. Im Falle von Widersprüchen zwischen diesem Verfahren und einer spezifischen Datenschutzbestimmung ist die spezifische Datenschutzbestimmung maßgeblich. Tools und Datenbanken, die nicht unter eine spezifische Datenschutzbestimmung fallen, unterliegen ausschließlich diesem Verfahren.

Dieses Verfahren wurde im Rahmen der Richtlinie (EU) 95/46 als "verbindliche unternehmensinterne Vorschriften" von ArcelorMittal aufgestellt.

Fragen zur Einhaltung dieses Verfahrens und/oder spezifischer Datenschutzbestimmungen können an den entsprechenden Datenschutzkorrespondenten (siehe Anhang VI) gerichtet werden.

Das Datum des Inkrafttretens dieses Verfahrens bei den Tochtergesellschaften ist abhängig von der Ausfertigung der unterzeichneten Fassung des Verfahrens zum Datenschutz durch die jeweilige Tochtergesellschaft.

Artikel 2 - Umfang des Verfahrens

Dieses Verfahren erstreckt sich auf:
(i) alle personenbezogenen Daten, die in der EU durch oder im Namen von ArcelorMittal verarbeitet werden, einschließlich der personenbezogenen Daten von Mitarbeitern, Kunden und Lieferanten
und
(ii) alle personenbezogenen Daten, die in der EU durch oder im Namen von ArcelorMittal verarbeitet und außerhalb der EU weitergeleitet oder zugänglich gemacht werden, einschließlich der personenbezogenen Daten von Mitarbeitern, Kunden und Lieferanten

Dieses Verfahren erstreckt sich auf alle Personen, deren Daten verarbeitet werden, ungeachtet ihrer Nationalität.

Dieses Verfahren erstreckt sich nicht auf anonymisierte Daten. Anonymisierte Daten sind Daten, anhand derer die einzelnen Personen weder direkt noch indirekt bestimmbar sind.

Dieses Verfahren erstreckt sich nicht auf Daten, die von Anfang an außerhalb der EU lokal von einer Tochtergesellschaft verarbeitet und weder vollständig noch teilweise an einen Mitgliedsstaat der EU weitergeleitet werden. Diese personenbezogenen Daten sind gemäß den jeweils am Ort der Verarbeitung der personenbezogenen Daten geltenden Gesetzen zu verarbeiten.

Die Prozesse, die gegenwärtig im Anwendungsbereich des Verfahrens enthalten sind, werden in Anhang VIII dieses Verfahrens beschrieben.

Artikel 3 - Grundsätze für die Verarbeitung personenbezogener Daten

3.1. Rechtmäßigkeitskriterien

Die Verarbeitung personenbezogener Daten beruht auf der folgende Grundlage:

- Der Betroffene hat seine Zustimmung unmissverständlich erteilt; oder

- Die Verarbeitung ist zur Ausführung eines Vertrags erforderlich, an dem der Betroffene beteiligt ist, oder zur Ergreifung von Maßnahmen auf Anforderung des Betroffenen vor Abschluss eines Vertrags; oder

- Die Verarbeitung ist zur Erfüllung einer gesetzlichen Verpflichtung des Herrn der Daten erforderlich; oder

- Die Verarbeitung ist zum Schutz der grundlegenden Interessen des Betroffenen erforderlich; oder

- Die Verarbeitung ist zur Ausführung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung einer offiziellen Funktion des Herrn der Daten oder eines Dritten erforderlich, dem die Daten bekannt gegeben werden.
Personenbezogene Daten können außerdem verarbeitet werden (i) falls eine Tochtergesellschaft von ArcelorMittal per Gesetz oder auf gerichtlichem Wege dazu verpflichtet wird (ii) für Vollstreckungsbehörden oder sonstige Regierungsbeamte auf der Grundlage eines vollstreckbaren Ersuchen der Regierung, oder im Zusammenhang mit einer Untersuchung mutmaßlicher oder tatsächlicher illegaler Aktivitäten, (iii) wenn eine Offenlegung erforderlich oder zweckmäßig ist, weil die grundlegenden Interessen von ArcelorMittal oder die Integrität oder das physische oder psychische Wohl seiner Mitarbeiter betroffen sein könnte

oder

- Die Verarbeitung ist zur Verfolgung berechtigter Interessen durch den Herrn der Daten oder durch den oder die Dritten erforderlich, dem bzw. denen die Daten bekannt gegeben werden, sofern nicht das Interesse oder die geschützten Grundrechte und Grundfreiheiten der Betroffenen überwiegen.

3.2. Regeln für die Verarbeitung personenbezogener Daten

Personenbezogene Daten werden nach Treu und Glauben und auf rechtmäßige Weise verarbeitet.

Personenbezogene Daten werden für bestimmte rechtmäßige Zwecke erhoben und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Personenbezogene Daten müssen angemessen, sachdienlich und nicht übermäßig umfangreich für die Zwecke sein, für die sie erhoben und verwendet werden.

Personenbezogene Daten müssen sachlich richtig und, wenn nötig, auf dem neuesten Stand sein. Zur Berichtigung oder Löschung inkorrekter oder unvollständiger personenbezogener Daten werden angemessene Maßnahmen ergriffen.

Personenbezogene Daten werden unter Beachtung der gesetzlich vorgeschriebenen Aufbewahrungsfristen nur so lange gespeichert, wie dies für den Zweck, für den sie erhoben und verarbeitet wurden, erforderlich ist.

Für besondere Kategorien von Daten werden zusätzliche Schutzvorkehrungen nach Artikel 9 dieses Verfahrens getroffen.

Auf personenbezogene Daten haben nur Personen Zugriff, deren Funktion den Umgang mit diesen personenbezogenen Daten erfordert, und nur soweit sie von diesen Kenntnis haben müssen.

Anhang I enthält eine Checkliste von Fragen zur Verdeutlichung der vorstehenden Regeln.

Anhang II enthält Angaben zu den genauen Verfahren, die bei der Einrichtung eines neuen Informationssystems zu beachten sind und die Einhaltung der vorstehenden Regeln sicherstellen sollen.

3.3. Besondere Kategorien von Daten

Die Verarbeitung besonderer Daten ist untersagt, es sei denn:

- Der Betroffene hat seine ausdrückliche Zustimmung zur Verarbeitung dieser besonderen Daten erteilt, sofern diese nicht durch die anwendbaren Gesetze untersagt ist; oder

- Die Verarbeitung ist zur Ausführung von Pflichten und besonderen Rechten des Herrn der Daten im Bereich des Arbeitsrechts (z. B. Antidiskriminierung) erforderlich, sofern sie gemäß den angemessene Sicherheitsvorkehrungen vorsehenden Bestimmungen nach nationalem Recht zulässig ist; oder

- Die Verarbeitung ist zum Schutz der grundlegenden Interessen des Betroffenen oder, falls der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Zustimmung zu erteilen, einer anderen Person erforderlich; oder

- Die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch eine Stiftung (z. B. die ArcelorMittal Stiftung), einen Verband oder eine sonstige Organisation ohne Erwerbszweck mit Ausrichtung auf die Bereiche Arbeitsschutz oder soziale Verantwortung im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung nur auf die Mitglieder der Organisation oder auf Personen bezieht, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, und die Daten nicht ohne Zustimmung des Betroffenen an Dritte weitergegeben werden; oder

- Die Verarbeitung bezieht sich auf besondere Daten, die der Betroffene offenkundig öffentlich gemacht hat; oder

- Die Verarbeitung sensibler Daten ist zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich; oder

- Die Verarbeitung sensibler Daten ist zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich und die Verarbeitung dieser Daten erfolgt durch Angehörige der Gesundheitsberufe, die nach einzelstaatlichem Recht oder von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen dem Berufsgeheimnis unterliegen, oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen.

Artikel 4 - Sicherheit und Vertraulichkeit

4.1. IT-Grundschutzmaßnahmen von ArcelorMittal

Angemessene technische, physische und organisatorische Maßnahmen werden ergriffen, um unbefugten Zugriff auf Daten und deren unrechtmäßige Verarbeitung sowie den unautorisierten oder versehentlichen Verlust, die Vernichtung oder Beschädigung von Daten gemäß der detaillierten Beschreibung in Anhang III zu diesem Verfahren (IT-Grundschutzmaßnahmen von ArcelorMittal) zu verhindern.

Unter Berücksichtigung des Stands der Technik und der Kosten für deren Implementierung sollen diese Maßnahmen ein Maß an Sicherheit garantieren, das den Risiken im Zusammenhang mit der Verarbeitung und Art der zu schützenden Daten entspricht.

Alle globalen Tools, segmentspezifischen Prozesse und lokalen Softwareanwendungen, die in den Anwendungsbereich dieses Verfahrens fallen, müssen den IT-Grundschutzmaßnahmen von ArcelorMittal entsprechen.

Um sicherzustellen, dass alle zukünftigen Tools oder Prozesse diesem Standard entsprechen, werden die IT-Grundschutzmaßnahmen von ArcelorMittal als Teil der Spezifikationen aufgenommen (siehe Anhang II). Externe Berater, die als Benutzer Zugang zu den Systemen und Tools von ArcelorMittal haben, müssen sich dazu verpflichten, die IT-Grundschutzmaßnahmen von ArcelorMittal zu befolgen.

Die IT-Grundschutzmaßnahmen von ArcelorMittal werden durch das Data Protection Committee bei Bedarf aktualisiert.

Das so definierte Maß an Schutz und Sicherheit ist ein Mindeststandard, den alle Tochtergesellschaften von ArcelorMittal einführen müssen. Die Tochtergesellschaften von ArcelorMittal werden dazu angehalten, ggf. zusätzliche Sicherheitsmaßnahmen einzuführen.

Bei Fragen zur Einhaltung der IT-Grundschutzmaßnahmen von ArcelorMittal (Anhang III) wenden Sie sich an den zuständigen IT Compliance & Security Officer ("ITCS", siehe Anhang VI).

4.2. Sicherheitsverletzungen

Der Datenschutzkorrespondent und/oder der ITCS haben das Data Protection Committee unverzüglich über alle mutmaßlichen oder tatsächlichen Sicherheitsverletzungen oder vergleichbaren Vorfälle zu informieren, die die den Schutz oder die Sicherheit personenbezogener Daten gefährden oder gefährden könnten.

Die betreffenden Tochtergesellschaften von ArcelorMittal haben alle Maßnahmen zu ergreifen, um eine bekannte Sicherheitsverletzung oder eine versuchte Verletzung zu beheben und alle externen Anbieter zur umfassenden Kooperation nach Anweisung des Data Protection Committee zu veranlassen. Ein entsprechend vom Data Protection Committee aufgeforderter Datenschutzkorrespondent hat bei der Suche nach und Identifizierung von Sicherheitsverletzungen behilflich zu sein.

Die betreffenden Tochtergesellschaften von ArcelorMittal und der Datenschutzkorrespondent haben mit den Zivil- und Strafverfolgungsbehörden bei allen Untersuchungen oder

Maßnahmen im Zusammenhang mit einer solchen Verletzung oder versuchten Verletzung umfassend zu kooperieren.

Die Sicherheitsverletzung ist dann vom Data Protection Committee zu dokumentieren, damit die gewonnenen Erkenntnisse weitergegeben werden können und die IT-Grundschutzmaßnahmen von ArcelorMittal (falls erforderlich) entsprechend geändert wird.

Artikel 5 - Rechte des Betroffenen

5.1. Herr der Daten

Jede Tochtergesellschaft von ArcelorMittal ist für die Einhaltung dieses Verfahrens verantwortlich.

Jede Tochtergesellschaft von ArcelorMittal gilt als Herr der Daten für ihre Personaldaten, sofern nichts anderweitiges durch bestimmte Datenschutzbestimmungen vorgegeben oder vom Data Protection Committee genehmigt wird.

(Nur zur Information: für andere Informationssysteme als die Personalinformationssysteme kann die juristische Person, die nach den üblichen Praktiken von ArcelorMittal als "Geschäftsinhaber" auftritt, als Herr der Daten erachtet werden).

5.2. Transparenz und Recht auf Informationen

Dieses Verfahren ist jedem Betroffenen leicht zugänglich zu machen. Auf Anfrage ist eine Kopie in Papierform oder auf elektronischem Wege zur Verfügung zu stellen.

Der Betroffene muss über die Übermittlung und Verarbeitung seiner personenbezogenen Daten informiert werden.

Vor der Verarbeitung seiner Daten erhält der Betroffene die folgenden Informationen:
- Die Identität des Herrn der Daten und ggf. seines Vertreters,
- Den Verarbeitungszweck, für den die Daten bestimmt sind,
- Alle weiteren Informationen, wie z. B.:
i) die Empfänger oder Kategorien von Empfängern der Daten,
ii) sein Recht auf Zugang zu und Berichtigung der ihn betreffenden Daten.

Wurden die Daten nicht beim Betroffenen eingeholt, so gilt die Pflicht zur Information des Betroffenen nicht, wenn sich die Erteilung dieser Information als unmöglich erweist oder einen unverhältnismäßigen Aufwand bedeuten würde oder falls eine Aufzeichnung oder Offenlegung der Daten ausdrücklich gesetzlich vorgesehen ist.

5.3. Recht auf Zugang zu und Berichtigung, Löschung oder Sperrung von Daten

Jeder Betroffene hat das Recht, uneingeschränkt, in angemessenen Abständen und ohne übermäßige Verzögerung oder Kosten eine Kopie aller ihn betreffenden Daten, die verarbeitet werden, zu erhalten.

Zur Vermeidung von Zweifeln hat ein Betroffener nicht das Recht, auf personenbezogene Daten zuzugreifen, die sich nicht auf ihn beziehen.

Jeder Betroffene hat das Recht auf Berichtigung, Löschung oder Sperrung von Daten, insbesondere, wenn die Daten unvollständig oder inkorrekt sind.

Jeder Betroffene hat das Recht, jederzeit aus zwingenden und schutzwürdigen, sich aus ihrer besonderen Situation ergebenden Gründen gegen die Verarbeitung seiner personenbezogenen Daten Widerspruch einzulegen, sofern diese Verarbeitung nicht gesetzlich vorgeschrieben ist. Bei einem berechtigten Widerspruch ist die Verarbeitung einzustellen.

Jeder Betroffene hat das Recht, auf Antrag kostenfrei gegen die Verarbeitung seiner personenbezogenen Daten zu den Zwecken des Direktmarketing Widerspruch einzulegen.

Der Betroffene kann durch Anfrage an den betreffenden Herrn der Daten Zugang zu seinen personenbezogenen Daten erhalten. Der Herr der Daten kann Anfragen unberücksichtigt lassen, wenn diese offenkundig ungerechtfertigt sind.

5.4. Automatisierte Einzelentscheidungen

Bewertungen oder Entscheidungen in Bezug auf den Betroffenen, die erhebliche Auswirkungen auf diesen haben, werden nicht ausschließlich auf die automatisierte Verarbeitung seiner Daten gestützt, es sei denn, die Entscheidung:
- wird im Rahmen des Abschlusses oder der Erfüllung eines Vertrags getroffen, sofern dem Antrag des Betroffenen auf Abschluss oder Erfüllung des Vertrags stattgegeben wurde, oder seine berechtigten Interessen werden durch geeignete Maßnahmen gewahrt, z. B. die Möglichkeit, seinen Standpunkt geltend zu machen; oder
- wird durch ein Gesetz zugelassen, das Maßnahmen zur Wahrung der berechtigten Interessen des Betroffenen festlegt.

Artikel 6 - Datenübermittlung

Personenbezogene Daten können mit Informationssystemen verarbeitet werden, die sich im Besitz eines externen Auftragsverarbeiters befinden und von diesem kontrolliert werden.

Vor der Übermittlung personenbezogener Daten an einen solchen Anbieter muss die betreffende Tochtergesellschaft von ArcelorMittal einen Anbieter auswählen, der im Hinblick auf die technischen Sicherheitsmaßnahmen und die organisatorischen Maßnahmen zur Regelung der auszuführenden Verarbeitung hinreichende Garantien bietet, und hat die Einhaltung dieser Maßnahmen sicherzustellen.

6.1. Datenübermittlung an externe Auftragsverarbeiter ("Anbieter") in der EU oder außerhalb der EU

Goldene Regel 1: Personenbezogene Daten von ArcelorMittal werden nicht ohne einen schriftlichen, von der betreffenden Tochtergesellschaft von ArcelorMittal und dem externen Auftragsverarbeiter unterschriebenen Vertrag an den externen Auftragsverarbeiter übermittelt oder diesem zugänglich gemacht. Ein solcher Vertrag enthält die diesem Verfahren beigefügten Standardvertragsbestimmungen (siehe Anhang V).

Goldene Regel 2: Personenbezogene Daten von ArcelorMittal werden nur an den externen Auftragsverarbeiter übermittelt oder diesem zugänglich gemacht, wenn dieser externe Auftragsverarbeiter ein Maß an Schutz bietet, das dem der IT-Grundschutzmaßnahmen von ArcelorMittal entspricht.

Goldene Regel 3: Bei grenzüberschreitenden Datenübermittlungen von Europa in ein anderes Land außerhalb Europas sind die neuesten Standardvertragsbestimmungen, die von der europäischen Gesetzgebung (Standardvertragsbestimmungen für die grenzüberschreitende Übermittlung personenbezogener Daten vom Herrn der Daten an den Auftragsverarbeiter) oder von nationalem Recht vorgegebenen werden, ebenfalls in den Vertrag aufzunehmen, der zwischen der betreffenden Tochtergesellschaft von ArcelorMittal und dem Auftragsverarbeiter geschlossen wird, wenn diese Anwendung finden.

Die in diesem Abschnitt beschriebene Sicherheitsbewertung ist vor Unterzeichnung des Vertrags (oder Vertragsverlängerung) in allen Szenarien vorzunehmen, in denen ein externer Auftragsverarbeiter Zugriff auf personenbezogene Daten hat.

Zweck der Sicherheitsbewertung ist folgender: der externe Auftragsverarbeiter muss das gleiche Maß an Schutz für die personenbezogenen Daten von ArcelorMittal bieten, wie die IT-Grundschutzmaßnahmen von ArcelorMittal.

Vor der Übermittlung personenbezogener Daten an einen Anbieter, der keine Tochtergesellschaft von ArcelorMittal ist, sind von der Tochtergesellschaft von ArcelorMittal, die die Funktion des Herrn der Daten übernimmt, die folgenden Maßnahmen zu ergreifen:

→ Maßnahme 1: Sicherheitsbewertung

Die betreffende Tochtergesellschaft von ArcelorMittal hat dem Anbieter, der Leistungen für ArcelorMittal erbringen möchte, den folgenden Fragebogen zur Sicherheitsbewertung (Anhang IV) zuzusenden.

Die Antworten des Anbieters sind vom IT Compliance & Security Officer zu prüfen, damit beurteilt werden kann, ob das von diesem Anbieter gebotene Maß an Schutz dem der IT-Grundschutzmaßnahmen von ArcelorMittal (Anhang III) entspricht.
Im Rahmen seiner Beurteilung erhält der IT Compliance & Security Officer von der Tochtergesellschaft von ArcelorMittal die Gelegenheit zu einem Gespräch mit dem Anbieter, er kann Verbesserungen zu den Sicherheitsmaßnahmen des Anbieters vorschlagen und dessen Systeme besichtigen um zu prüfen, ob der Anbieter tatsächlich ein gleichwertiges Maß an Schutz bietet.

Fällt das Ergebnis der Bewertung wegen eines kritischen Problems im Zusammenhang mit den Richtlinien des Anbieters negativ aus, so werden die Verhandlungen ausgesetzt und es kommt nicht zu einer Vertragsunterzeichnung, bis der Anbieter sich verpflichtet, das Problem/die Probleme, das/die vom ITCS angesprochen wurden, innerhalb kurzer Zeit zu lösen.

→ Maßnahme 2: Vertrag

Falls der ITCS die Antworten des Anbieters auf den Fragebogen zur Sicherheitsbewertung für zufriedenstellend befindet, werden diese Antworten in den zwischen der Tochtergesellschaft von ArcelorMittal und dem Anbieter geschlossenen Vertrag aufgenommen. Die Antworten werden zu einem wesentlichen Bestandteil des Vertrags.

In den zwischen der betreffenden Tochtergesellschaft von ArcelorMittal und dem externen Auftragsverarbeiter geschlossenen Vertrag werden außerdem die diesem Verfahren beigefügten Standardbestimmungen (siehe Anhang V) aufgenommen. Falls und soweit die Datenschutzgesetze allerdings strengere Verpflichtungen für einen solchen Vertrag vorsehen, sind die Datenschutzgesetze maßgeblich, so dass die in Anhang V enthaltenen Standardbestimmungen, die im Widerspruch zu den entsprechenden Datenschutzgesetzen stehen, durch neue Bestimmungen ersetzt werden, die diesen Datenschutzgesetzen entsprechen.

Bei grenzüberschreitenden Datenübermittlungen von Europa in ein anderes Land außerhalb Europas sind die neuesten Standardvertragsbestimmungen, die von der europäischen Gesetzgebung (Standardvertragsbestimmungen für die grenzüberschreitende Übermittlung personenbezogener Daten vom Herrn der Daten an den Auftragsverarbeiter) oder von nationalem Recht vorgegebenen werden, ebenfalls in den Vertrag aufzunehmen, der zwischen der betreffenden Tochtergesellschaft von ArcelorMittal und dem Auftragsverarbeiter geschlossen wird, wenn diese Anwendung finden.

6.2. Datenübermittlungen an den ArcelorMittal Auftragsverarbeiter

Jeder ArcelorMittal Auftragsverarbeiter muss die IT-Grundschutzmaßnahmen von ArcelorMittal befolgen.

Die IT-Grundschutzmaßnahmen von ArcelorMittal werden automatisch in alle Verträge aufgenommen, die zwischen einem ArcelorMittal Auftragsverarbeiter und seinen Kunden (d. h. den Herrn der Daten) geschlossen werden.

Der Zweck, für den die personenbezogenen Daten von dem ArcelorMittal Auftragsverarbeiter im Namen seines Kunden verarbeitet werden sollen, ist zwischen dem ArcelorMittal Auftragsverarbeiter und seinem ArcelorMittal Kunden zu vereinbaren. Der ArcelorMittal Auftragsverarbeiter darf die personenbezogenen Daten zu keinem anderen Zweck verarbeiten. Der ArcelorMittal Auftragsverarbeiter darf die personenbezogenen Daten nur entsprechend den schriftlichen Anweisungen seines Kunden übermitteln.

Bei der teilweisen oder vollständigen Weitervergabe der zu erbringenden Leistungen an einen externen Auftragsverarbeiter, hat der ArcelorMittal Auftragsverarbeiter den in Abschnitt 6.1 oben beschriebenen Ablauf zu befolgen.

6.3. Datenübermittlung an externe Herren der Daten

Jede Übermittlung personenbezogener Daten von Europa an externe Herren der Daten mit Sitz außerhalb der EU müssen den europäischen Bestimmungen für grenzüberschreitende Datenübermittlungen entsprechen (Paragraph 25-26 der Richtlinie 95/46/EG: z. B. indem die EU-Standardvertragsbestimmungen verwendet werden, die durch die Entscheidungen der Europäischen Kommission 2001/497/EG oder 2004/915/EG oder entsprechende andere vertragliche Instrumente gemäß Paragraph 25 und 26 der EU-Richtlinie genehmigt wurden).

6.4. Datenübermittlung an eine neue Tochtergesellschaft von ArcelorMittal

Personenbezogenen Daten dürfen an eine neue Tochtergesellschaft von ArcelorMittal erst übermittelt werden, wenn (i) dieses Verfahren von dieser neuen Tochtergesellschaft unterzeichnet wurde und (ii) ein neuer Datenschutzkorrespondent ernannt wurde, falls es im betreffenden Land/Segment keinen Datenschutzkorrespondenten gibt.

Artikel 7 - Umsetzung dieses Verfahrens und Durchsetzungsmechanismen

- Einhaltung der Bestimmungen auf lokaler/regionaler Ebene (Datenschutzkorrespondent und ITCS)
- Data Protection Committee von ArcelorMittal
- Schulungsprogramm
- Interner Beschwerdemechanismus
- Prüfprogramm
- Gegenseitige Unterstützung und Kooperation mit den Datenschutzbehörden
- Ergreifung von Maßnahmen, falls die nationalen Gesetze die Befolgung dieses Verfahrens verhindern

7.1. Einhaltung der Bestimmungen auf lokaler/regionaler Ebene (Datenschutzkorrespondent und ITCS)

Datenschutzkorrespondent

Jeder Country Manager oder Segment Manager von ArcelorMittal ernennt einen oder mehrere Datenschutzkorrespondenten. Jedem Datenschutzkorrespondenten wird ein genauer geographischer und/oder organisatorischer Kompetenzbereich zugewiesen.

Der Datenschutzkorrespondent koordiniert alle Maßnahmen, die dazu erforderlich sind sicherzustellen, dass die Tochtergesellschaften in seinem Kompetenzbereich ihren Verpflichtungen im Rahmen dieses Verfahrens nachkommen.

Der Datenschutzkorrespondent ist außerdem der Hauptansprechpartner für alle Beschwerden, die in seinem Kompetenzbereich gemäß der Beschreibung in Abschnitt 7.4 dieses Verfahrens ("Interner Beschwerdemechanismus") auftreten, sowie für alle Sicherheitsverletzungen gemäß der Beschreibung in Abschnitt 4.2 dieses Verfahrens ("Sicherheitsverletzung").

Der Datenschutzkorrespondent hat die Pflicht, mit den anderen Datenschutzkorrespondenten in jeder Angelegenheit im Zusammenhang mit der ordnungsgemäßen Durchführung dieses Verfahrens umfassend zusammenzuarbeiten, insbesondere in Angelegenheiten, an denen mehrere Herren der Daten in verschiedenen Ländern/Segmenten beteiligt sind, oder die sich auf mehrere Herren der Daten in verschiedenen Ländern/Segmenten auswirken.

Der Datenschutzkorrespondent informiert das Data Protection Committee kontinuierlich über alle Beschwerden oder sonstigen Fragen/Probleme, die im Rahmen dieses Verfahrens entstehen.

Sollte ein Datenschutzkorrespondent seinen Pflichten nicht nachkommen, kann der Datenschutzkorrespondent vom Data Protection Committee von seinem Amt abberufen werden. In diesem Fall wird ein neuer Datenschutzkorrespondent vom Country Manager oder der Geschäftsführung vor Ort ernannt.

IT Compliance and Security (ITCS) Team

Die Aufgabe der IT Compliance & Security Officers ist es, den Einsatz interner Kontrollsysteme innerhalb der ArcelorMittal IT, die zum Erreichen der IT-Ziele in den Bereichen Einhaltung der Bestimmungen und Sicherheit erforderlich sind, zu definieren, zu implementieren und zu überwachen.

Die ITCS Officers implementieren und überwachen insbesondere den Einsatz der IT-Grundschutzmaßnahmen von ArcelorMittal, sowohl intern, als auch im Hinblick auf externe Auftragsverarbeiter durch Überprüfung eines entsprechenden Mindestmaßes an Sicherheit gemäß Abschnitt 6.1 dieses Verfahrens.

7.2. Data Protection Committee von ArcelorMittal

Das Data Protection Committee wurde für die Dauer dieses Verfahrens gebildet.

Das Data Protection Committee besteht aus drei (3) Kernmitgliedern,

. eines (1), das vom Group CIO von ArcelorMittal ernannt wird,

. eines (1), das vom EVP Human Resource von ArcelorMittal ernannt wird,

. und einem Schriftführer, der vom Group General Counsel von ArcelorMittal ernannt wird.

Die anfänglichen Mitglieder des Data Protection Committee werden in Anhang IX genannt.

Zum Data Protection Committee gehören auch alle oder einige Datenschutzkorrespondenten, soweit dies von den Kernmitgliedern zur effektiven Behandlung der auf der jeweiligen Tagesordnung stehenden Punkte als erforderlich erachtet wird.

Darüber hinaus kann der Leiter der Abteilung Internal Assurance von ArcelorMittal nach seinem eigenen Ermessen selbst an den Versammlungen des Data Protection Committee teilnehmen oder einen Vertreter entsenden.

Jedes Mitglied kann nach eigenem Ermessen andere Mitglieder oder Berater zur Teilnahme an den Versammlungen des Data Protection Committee einladen. Zur Vermeidung von Zweifeln wird darauf hingewiesen, dass sich kein eingeladener Berater an einer Entscheidung beteiligen darf oder als Mitglied des Data Protection Committee von ArcelorMittal erachtet wird.

Der Group CIO, der EVP Human Resource and der Group General Counsel können jederzeit die Ernennung des/der von ihnen ernannten Mitglieds/Mitglieder zurückziehen und einen Ersatz (dessen Amtszeit sofort beginnt) ernennen, indem sie den anderen Mitgliedern eine Mitteilung über die Zurückziehung und den Ersatz erteilen.

Das Data Protection Committee tritt an den Terminen und Orten zusammen, die von den Mitgliedern des Data Protection Committee jeweils vereinbart werden, jedoch mindestens einmal alle drei (3) Monate.

Die Tagesordnung für jede Versammlung wird vom Schriftführer aufgestellt und den Mitgliedern des Data Protection Committee sowie den Datenschutzkorrespondenten mitgeteilt.

Der Schriftführer des Data Protection Committee hat innerhalb von drei (3) Werktagen nach jeder Versammlung des Data Protection Committee einen detaillierten schriftlichen Bericht der bei der Versammlung gefassten Beschlüsse aufzustellen und den Mitgliedern des Data Protection Committee zuzusenden.

Dieser Bericht ist ebenfalls an die Datenschutzkorrespondenten zu übermitteln.

Aufgaben des Data Protection Committee:

(i) die Liste der diesem Verfahren unterliegenden ArcelorMittal Tochtergesellschaften führen und aktualisieren,

(ii) die Liste der Datenschutzkorrespondenten gemäß den Anforderungen der ArcelorMittal Manager auf lokaler/regionaler Ebene führen und aktualisieren (siehe ursprüngliche Liste in Anhang VI),

(iii) die Umsetzung dieses Verfahrens und dessen Durchführung durch die Tochtergesellschaften, einschließlich der zukünftigen Tochtergesellschaften von ArcelorMittal beaufsichtigen,

(iv) wichtige Fragen/Probleme klären, die entstehen können,

(v) besondere Richtlinien für globale Tools aufstellen, prüfen und aktualisieren (derartige Richtlinien sind nur mit vorheriger Zustimmung des Data Protection Committee durchsetzbar),

(vi) Anhang II und Anhang III, IV, V, VI, VII und VIII mit umfassender Befugnis aktualisieren. Eine entsprechende Änderung ist den Datenschutzkorrespondenten und dem ITCS mitzuteilen und wird an dem in der Mitteilung genannten Datum verbindlich. So wird z. B. erwartet, dass die in Anhang V enthaltenen Standardvertragsbestimmungen für externe Anbieter je nach Land an die nationalen Gesetze und deren jeweilige Fassungen angepasst werden müssen.

(vii) dieses Verfahren bei Bedarf modifizieren, z. B. um Änderungen in Gesetzen, Verordnungen, Praktiken und Verfahren, der Unternehmensstruktur von ArcelorMittal oder den Anforderungen der Datenschutzbehörden nachzukommen. Änderungen an diesem Kerndokument sind den Tochtergesellschaft von ArcelorMittal mitzuteilen und werden nach einem Zeitraum von zwei (2) Monaten als von diesen akzeptiert erachtet, sofern sie nicht von einer Tochtergesellschaft ausdrücklich schriftlich abgelehnt werden.

(viii) sicherstellen, dass Änderungen an diesem Kerndokument und Änderungen an den Liste der diesem Verfahren unterliegenden Tochtergesellschaften von ArcelorMittal den genehmigenden Datenschutzbehörden mit einer kurzen Erklärung der Gründe für diese Änderungen mitgeteilt werden.

(ix) alle Versionen dieses Verfahrens verwalten

7.3 Schulungsprogramm

Den Mitarbeitern, die ständigen oder regelmäßigen Zugang zu personenbezogenen Daten haben, in die Erfassung personenbezogener Daten oder in die Entwicklung von Tools zur Verarbeitung personenbezogener Daten eingebunden sind, werden entsprechende Schulungen zu diesem Verfahren angeboten.

Für dieses Schulungsprogramm, das in Form einer e-Learning-Lösung durchgeführt werden kann, ist der Datenschutzkorrespondent zuständig.

7.4 Interner Beschwerdemechanismus

Betroffene können sich darüber beschweren, dass ein Herr der Daten von ArcelorMittal dieses Verfahren nicht befolgt.

Der Datenschutzkorrespondent des betreffenden Herr der Daten von ArcelorMittal ist für die zeitnahe Bearbeitung einer solchen Beschwerde zuständig. Ein erstes Feedback erhält der Beschwerdeführer innerhalb von einem (1) Monat nach der Beschwerde. Der Datenschutzkorrespondent unternimmt unter Berücksichtigung der Komplexität und des

Umfangs der Beschwerde alle Anstrengungen, um die Beschwerde zeitnah zu bearbeiten. Den Erwartungen zufolge dauern Untersuchungen zwischen einem (1) und sechs (6) Monaten, es sei denn, es liegen unübliche Umstände oder Ausnahmefälle vor.

Falls ein Problem nicht vom Datenschutzkorrespondenten gelöst werden kann, eskaliert er dieses Problem an das Data Protection Committee von ArcelorMittal.

Der Betroffene kann jederzeit eine Beschwerde vor der zuständigen Datenschutzbehörde erheben oder am Gerichtsstand eines in der EU ansässigen Datenexporteurs Klage einreichen.

7. 5 Prüfplan

Die Einhaltung dieses Verfahrens durch den Konzern wird regelmäßig von der Abteilung Internal Assurance überprüft. Die Prüfungen finden mindestens zweimal jährlich statt. Die Abteilung Internal Assurance kann von einem Mitglied des Data Protection Committee unterstützt werden. Darüber hinaus kann ein externes Team bestellt werden.

Eine solche Prüfung kann sich auf alle Aspekte dieses Verfahrens, sowohl innerhalb als auch außerhalb Europas, beziehen.

Zu jeder Prüfung wird ein Bericht, falls nötig unter detaillierter Angabe von Korrekturmaßnahmen, erstellt (Phase 1). Diese Maßnahmen werden innerhalb eines bestimmten, in dem Bericht angegebenen Zeitrahmens von der/den Tochtergesellschaft(en) von ArcelorMittal durchgeführt. Bei einem zweiten Besuch wird dann sichergestellt, dass alle Korrekturmaßnahmen umgesetzt wurden (Phase 2).

Die Abteilung Internal Assurance und das Data Protection Committee stellen einen jährlichen Prüfplan auf.

Eine Kopie aller Prüfberichte ist (i) dem/den betreffenden Datenschutzkorrespondenten, (ii) dem Data Protection Committee, (iii) dem EVP Human Resource, dem Group CIO und dem Group General Counsel und (iv) der Geschäftsführung der betreffenden Tochtergesellschaft(en) zu übermitteln.
Die Datenschutzbehörden erhalten auf Anforderung Zugang zu den Prüfberichten.

Die Prüfberichte dürfen keiner nicht in diesem Abschnitt 7.5 ("Prüfplan") genannten Stelle oder Person übermittelt werden.

7.6. Gegenseitige Unterstützung und Kooperation mit den Datenschutzbehörden

- Die Tochtergesellschaften haben bei der Bearbeitung von Anträgen oder Beschwerden eines Betroffenen oder einer Untersuchung oder Anfrage der Datenschutzbehörden zu kooperieren und sich gegenseitig zu unterstützen.

- Im Falle eines Verstoßes gegen dieses Verfahren außerhalb von Europa, kann die Datenschutzbehörde in dem Land, in dem der Datenexporteur ansässig ist, die Durchführung

einer Prüfung durch die Abteilung Internal Assurance von ArcelorMittal verlangen. Eine solche Prüfung ist gemäß Abschnitt 7.5 dieses Verfahrens durchzuführen.

- Die Tochtergesellschaften haben den Rat der Datenschutzbehörden zu allen Fragen im Zusammenhang mit der Auslegung dieses Verfahrens zu befolgen.

7.7 Ergreifung von Maßnahmen, falls die nationalen Gesetze die Befolgung dieses Verfahrens verhindern

Hat eine Tochtergesellschaft Grund zu der Annahme, dass der Herr der Daten seinen Pflichten im Rahmen dieses Verfahrens aufgrund der auf ihn anwendbaren Gesetze, die sich wesentlich auf die von diesem Verfahren gewährten Garantien auswirken, nicht nachkommen kann, hat er das Data Protection Committee unverzüglich zu informieren (es sei denn, dies wäre von einer Strafverfolgungsbehörde untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen).

Darüber hinaus wird das Data Protection Committee bei einem Widerspruch zwischen nationalem Recht und den in diesem Verfahren vorgesehenen Verpflichtungen eine angemessene Entscheidung über die zu ergreifenden Maßnahmen treffen und im Zweifelsfalls die zuständigen Datenschutzbehörden zu Rate ziehen.

Artikel 8 - Haftung

Ein Betroffener kann die folgenden Grundsätze vor den entsprechenden Datenschutzbehörden oder vor einem Gericht als Rechte durchsetzen, um einen Rechtsschutz zu erwirken und eine Entschädigung zu erhalten, falls eine der Tochtergesellschaften diese Grundsätze nicht befolgt:

- Nationale Gesetze, die die Befolgung dieses Verfahrens gemäß Artikel 7.7 dieses Verfahrens verhindern,
- Das Recht zur Führung von Beschwerden durch den in Artikel 7.4 beschriebenen internen Beschwerdemechanismus,
- Die in Artikel 7.6 beschriebene Pflicht zur Kooperation mit den Datenschutzbehörden,
- Die Bestimmungen zu Haftung und Gerichtstand gemäß den folgenden Absätzen und Artikel 7.4,
- Einschränkung des Verarbeitungszwecks gemäß Artikel 3.2,
- Die Eigenschaft der Daten und die Verhältnismäßigkeit der Datenerfassung gemäß Artikel 3.2,
- Kriterien für die Legitimierung der Verarbeitung gemäß Artikel 3.1,
- Transparenz und leichter Zugang zu diesem Verfahren gemäß Artikel 5.2,
- Recht auf Zugang zu und Berichtigung, Löschung oder Sperrung von Daten und Widerspruch gegen die Verarbeitung gemäß Artikel 5.3,
- Rechte im Falle automatisierter Einzelentscheidungen gemäß Artikel 5.4,
- Sicherheit und Vertraulichkeit gemäß Artikel 4,
- Einschränkungen für die Weiterleitung an Empfänger, die nicht zu den Konzerngesellschaften gehören, gemäß Artikel 6.1 und 6.3.

Jede Tochtergesellschaft von ArcelorMittal übernimmt die Verantwortung für jeden Verstoß gegen dieses Verfahren, ungeachtet der in Artikel 8.2 beschriebenen gemeinsamen Haftung für Verstöße.

Der Betroffene kann gemäß Artikel 7.4 jederzeit eine Beschwerde vor der zuständigen Datenschutzbehörde erheben oder am Gerichtsstand eines in der EU ansässigen Datenexporteurs Klage einreichen.

Diese Rechte erstrecken sich nicht auf die Elemente dieses Verfahrens, die zu dem innerhalb der Tochtergesellschaften eingesetzten internen Mechanismus gehören, wie z. B. Einzelheiten zu den Schulungs- und Prüfprogrammen, dem Netzwerk der Compliance-Beauftragten und dem Mechanismus zur Aktualisierung der Bestimmungen.

8.1. Pflicht zur Behebung von Verstößen

Sollte eine Tochtergesellschaft von ArcelorMittal gegen dieses Verfahren verstoßen, so hat diese den Verstoß verursachende Tochtergesellschaft von ArcelorMittal den Verstoß zu beheben und alle erforderlichen Maßnahmen zur Befolgung dieses Verfahrens zu ergreifen.

Die Tochtergesellschaften sichern zu, jeden Verstoß, Verzug und jede Nichtbefolgung dieses Verfahrens zu beheben, um zukünftig ein erneutes Auftreten des Problems zu vermeiden.

8.2. Verpflichtung zur Leistung von Schadenersatz an den Betroffenen

Darüber hinaus hat jeder Betroffene, der infolge eines Verstoßes gegen die acht (8) vorstehend aufgelisteten Rechte des Betroffenen einen Schaden erlitten hat, Anspruch auf eine Entschädigung für den erlittenen Schaden.

Falls die Tochtergesellschaft, die den Verstoß verursacht hat, nicht in Europa ansässig ist, finden die folgenden Regeln Anwendung:

- die Tochtergesellschaft, die den Verstoß verursacht hat, und der Datenexporteur haften gesamtschuldnerisch für alle Schäden, die dem Betroffenen infolge eines Verstoßes gegen die Bestimmungen dieses Verfahrens entstanden sind.
- Die Tochtergesellschaft, die den Verstoß verursacht hat, hat den Datenexporteur für alle ihm entstandenen Kosten, Gebühren, Schadenersatzzahlungen, Aufwendungen oder Verluste zu entschädigen.
- Falls der Datenexporteur nachweisen kann, dass das außerhalb Europas ansässige Mitglied nicht für den Verstoß verantwortlich ist, kann er sich selbst von jeglicher Verantwortung befreien.

ANHANG I

GRUNDSÄTZE FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN

CHECKLISTE

Zweck dieser Checkliste ist es zu verdeutlichen, wie die Datenschutzgrundsätze zu verstehen sind.

"Personenbezogene Daten werden nach Treu und Glauben und auf rechtmäßige Weise verarbeitet"

- Gibt es eine klare unternehmerische Notwendigkeit für die Verarbeitung dieser Daten?

- Wissen die Personen, deren Daten ich besitze, dass ich sie habe, und verstehen sie, für welchen Zweck diese verwendet werden?

- Muss ich die Datenschutzbehörde informieren und falls ja, ist meine Mitteilung aktuell?

"Personenbezogene Daten werden für bestimmte rechtmäßige Zwecke erhoben und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden"

- Weiß ich, wofür ich diese personenbezogenen Daten verwenden werde?

- Falls ich gebeten werde, personenbezogene Daten weiterzuleiten: würden die Personen, deren Daten ich besitze, das von mir erwarten?

"Personenbezogene Daten müssen angemessen, sachdienlich und nicht übermäßig umfangreich für die Zwecke sein, für die sie erhoben und verwendet werden"

- Brauche ich diese Daten wirklich über eine Person?

"Personenbezogene Daten müssen sachlich richtig und, wenn nötig, auf dem neuesten Stand sein. Zur Berichtigung oder Löschung inkorrekter oder unvollständiger personenbezogener Daten werden angemessene Maßnahmen ergriffen"

- Bin ich sicher, dass die personenbezogenen Daten richtig und aktuell sind?

"Personenbezogene Daten werden unter Beachtung der gesetzlich vorgeschriebenen Aufbewahrungsfristen nur so lange gespeichert, wie dies für den Zweck, für den sie erhoben und verarbeitet wurden, erforderlich ist"

- Soll ich personenbezogene Daten löschen oder vernichten, sobald ich sie nicht mehr benötige?

"Sensible Daten unterliegen zusätzlichen Sicherheitsvorkehrungen, wie z. B. den Bestimmungen der Richtlinie (EU) 95/46/EG"

- Habe ich meine Mitarbeiter gemäß dem Verfahren von ArcelorMittal zum Datenschutz in Bezug auf ihre Aufgaben und Verantwortungsbereiche geschult und setzen sie die Vorgaben um?

"Auf personenbezogene Daten haben nur Personen Zugriff, zu deren Funktion der Umgang mit diesen personenbezogenen Daten gehört, und nur soweit sie von diesen Kenntnis haben müssen"

- Ist der Zugang zu den personenbezogenen Daten auf die Personen beschränkt, die diese unbedingt kennen müssen?

- Bin ich davon überzeugt, dass die Daten sicher aufbewahrt werden?

ANHANG II

DATENSCHUTZ-CHECKPUNKT VOR ABSCHLUSS DER DESIGNPHASE EINES PROJEKTES

Die Designphase eines Projektes ist von äußerster Wichtigkeit um sicherzustellen, dass die sich ergebenden Prozesse/Anwendungen diesem Verfahren entsprechen. "Designphase" ist die Phase, in der die Architektur, die Spezifikationen und die Funktionen des Systems vom Projektteam im Namen des/der Herr(e)n der Daten definiert werden.

Die in diesem Verfahren dargelegten Grundsätze sind bereits in der Designphase in ein neues Informationssystem oder in dessen wesentliche Versionen zu integrieren.

Dieser ANHANG beschreibt, wie dieses Ziel zu erreichen ist.

Einleitend muss angemerkt werden, dass dieses Verfahren technologieneutral ist. Falls ein bestehendes System auf der Grundlage einer neuen Technologie neu entwickelt wird, während die gleichen Prozesse, die gleichen Daten, die gleichen Organisations- und Sicherheitsmaßnahmen beibehalten werden, sind die zum Zeitpunkt des Designs des bestehenden Systems ausgesprochenen Empfehlungen zu befolgen, aber für diese Neuentwicklung wird kein neuer Datenschutz-Checkpoint benötigt.

Dieser ANHANG gilt für alle neuen Informationssysteme, die diesem Verfahren unterliegen, oder für alle Versionen dieser Informationssysteme (sofern sich die Art und Weise der Verarbeitung personenbezogener Daten ändert).

- Neues globales Tool

Das Data Protection Committee ist von dem Projektteam vor der Validierung des Designs eines neuen globalen Tools zu konsultieren.
Das Data Protection Committee wird das Projektteam beraten und dabei unterstützen sicherzustellen, dass das Systemdesign diesem Verfahren entspricht.
In jedem Fall sind die IT-Grundschutzmaßnahmen (siehe ANHANG III) in die Spezifikationen aufzunehmen.

- Segmentspezifische Prozesse

Die Datenschutzkorrespondenten der betreffenden Länder sind von dem Projektteam vor der Validierung des Designs neuer segmentspezifischer Prozesse zu konsultieren.
Die Datenschutzkorrespondenten werden das Projektteam beraten und dabei unterstützen sicherzustellen, dass das Systemdesign diesem Verfahren entspricht.
In jedem Fall sind die IT-Grundschutzmaßnahmen (siehe ANHANG III) in die Spezifikationen aufzunehmen.
Falls mit dem neuen System personenbezogene Daten aus einem bereits bestehenden Tool oder Prozess übernommen werden sollen, hat das Projektteam auch das Data Protection Committee zu Rate zu ziehen.

- Lokale Softwareanwendungen

Der Datenschutzkorrespondent des betreffenden Landes muss vor der Validierung des Systemdesigns zu Rate gezogen werden.

Der Datenschutzkorrespondent wird das Projektteam beraten und dabei unterstützen sicherzustellen, dass das Systemdesign diesem Verfahren entspricht.
In jedem Fall sind die IT-Grundschutzmaßnahmen (siehe ANHANG III) in die Spezifikationen aufzunehmen.
Falls mit den neuen Softwareanwendungen personenbezogene Daten aus einem bereits bestehenden System übernommen werden sollen, ist auch das Data Protection Committee zu Rate zu ziehen.

Diese Vorschrift kann je nach Einzelfall oder Anwendung verschiedene Maßnahmen nach sich ziehen. In einigen Fällen kann z. B. die Löschung/Reduzierung personenbezogener Daten oder die Vermeidung einer unnötigen Verarbeitung oder die Verbesserung der Sicherheitsmaßnahmen erforderlich sein, um den IT-Grundschutzmaßnahmen zu entsprechen.

Der/die Herr(e)n der Daten ist/sind für die Umsetzung der Systemempfehlungen des Datenschutzkorrespondenten zuständig.

Aktuelle Version der Bestimmungen: http://www..... ArcelorMittal Intranet

ANHANG III

IT-GRUNDSCHUTZMAßNAHMEN

Aktuelle Version der Richtlinien: http://www..... ArcelorMittal Intranet

ANHANG IV

FRAGEBOGEN ZUR SICHERHEITSBEWERTUNG

Aktuelle Version des Fragebogens: http://www..... ArcelorMittal Intranet

ANHANG V

Standardvertragsbestimmungen von ArcelorMittal für externe Auftragsverarbeiter
Diese Bestimmungen sind VERBINDLICH in alle Verträge zwischen einer Tochtergesellschaft von ArcelorMittal in ihrer Eigenschaft als Herr der Daten und einem externen Auftragsverarbeiter in seiner Eigenschaft als Auftragnehmer aufzunehmen, dem die Tochtergesellschaft von ArcelorMittal zur Förderung des Vertragszwecks im Rahmen einer strukturierten Übermittlung europäischer personenbezogener Daten von der Tochtergesellschaft von ArcelorMittal an den externen Auftragsverarbeiter personenbezogene Daten bekannt geben wird, die diesem Verfahren unterliegen.
. Es wird davon ausgegangen, dass die Geschäftsvereinbarung, in die diese Bestimmungen aufgenommen werden, bereits eine klare Beschreibung (i) des Gesamtzwecks des Vertrags, (ii) der zu erbringenden Leistungen und (iii) der an den Auftragsverarbeiter zu übermittelnden oder diesem zugänglich zu machenden Daten enthält.

Dieser Anhang enthält außerdem eine Sonderversion für Deutschland (siehe unten).

Datenschutz

"Personenbezogene Daten" sind alle Daten über eine bestimmte oder bestimmbare natürliche Person, die (i) von ArcelorMittal oder einer Tochtergesellschaft von ArcelorMittal bereitgestellt werden und im Sinne dieser Vereinbarung in den Besitz eines Anbieters oder einer Tochtergesellschaft des Anbieters gelangen, (ii) die aus den von ArcelorMittal oder einer Tochtergesellschaft von ArcelorMittal im Sinne dieser Vereinbarung bereitgestellten Daten generiert werden oder entstehen und (iii) von den vom Anbieter für ArcelorMittal erbrachten Leistungen automatisch generiert werden.

[ArcelorMittal ist und bleibt der Herr der Daten und der Anbieter ist in Bezug auf die personenbezogenen Daten nur der Auftragsverarbeiter] (*). Der Anbieter verarbeitet personenbezogene Daten (einschließlich ursprünglich von ArcelorMittal verarbeiteter personenbezogener Daten) nur zur Erbringung der in dieser Vereinbarung beschriebenen Leistungen. Der Anbieter unternimmt alle Anstrengungen, um die Zuverlässigkeit der Mitarbeiter des Anbieters sicherzustellen, die Zugang zu den personenbezogenen Daten haben oder für deren Verarbeitung verantwortlich sind.
Bei Kündigung oder Ablauf dieser Vereinbarung oder auf schriftliche Anforderung von ArcelorMittal hin hat der Anbieter: (i) die Verarbeitung der personenbezogenen Daten sofort einzustellen; und (ii) die personenbezogenen Daten und alle Kopien, Anmerkungen oder Auszüge aus diesen innerhalb von sieben (7) Werktagen ab dem Datum der Kündigung oder des Ablaufs dieser Vereinbarung oder des Eingangs der Aufforderung an ArcelorMittal zurückzugeben oder auf Wunsch von ArcelorMittal zu vernichten. Auf Aufforderung durch ArcelorMittal hat der Anbieter außerdem schriftlich zu bestätigen, dass der Anbieter die in dieser Bestimmung dargelegten Pflichten erfüllt hat.

Der Anbieter hat jederzeit die dieser Vereinbarung beigefügten IT-Sicherheitsrichtlinien (**) und alle maßgeblichen Datenschutzgesetze und -verordnungen ("Datenschutzgesetze") zu befolgen. Falls und soweit die

Datenschutzgesetze dem Anbieter strengere Verpflichtungen, einschließlich strengerer Sicherheitsmaßnahmen, auferlegen als diese Vereinbarung, sind die Datenschutzgesetze maßgeblich.

Der Anbieter darf personenbezogene Daten nur mit vorheriger schriftlicher Zustimmung von ArcelorMittal Dritten, einschließlich der Tochtergesellschaften oder Subunternehmer ("Unterauftragsverarbeiter") des Anbieters, bekannt geben oder in sonstiger Form an diese übermitteln, und diese Zustimmung kann nach dem alleinigen Ermessen von ArcelorMittal aus jeglichem Grund oder unbegründet verweigert werden. Vor Einholung der Zustimmung von ArcelorMittal hat der Anbieter ArcelorMittal alle Einzelheiten der geplanten Beteiligung des Unterauftragsverarbeiters anzugeben, u. a. einschließlich der Identität des Unterauftragsverarbeiters, seiner Datenschutzhistorie, dem Standort seiner Verarbeitungseinrichtungen, einer Beschreibung des geplanten Zugangs zu den Daten von ArcelorMittal und allen sonstigen Informationen, die ArcelorMittal billigerweise anfordern kann, um die Risiken zu bewerten, die mit der Zulassung des Unterauftragsverarbeiters zur Verarbeitung der personenbezogenen Daten verbunden sind. Als Bedingung für die Erteilung seiner Zustimmung zu der geplanten Unterauftragsverarbeitung kann ArcelorMittal den Anbieter auffordern, eine schriftliche Vereinbarung mit dem Unterauftragsverarbeiter zu schließen, die dieser Vereinbarung entsprechende Bedingungen enthält (sofern der Anbieter nicht berechtigt ist, dem Unterauftragsverarbeiter die weitere Unterauftragsvergabe oder sonstige Delegierung der gesamten oder eines Teils der Verarbeitung des Unterauftragsverarbeiters ohne vorherige schriftliche Zustimmung von ArcelorMittal zu gestatten, die nach dem alleinigen Ermessen von ArcelorMittal erteilt werden kann).
Auf jeden Fall hat der Anbieter dafür Sorge zu tragen, dass sein autorisierter Unterauftragsverarbeiter die in dieser Vereinbarung enthaltenen Datenschutzverpflichtungen und alle maßgeblichen Datenschutzgesetze in jeglicher Hinsicht befolgt.

ArcelorMittal kann den Anbieter auffordern, zusätzliche Bedingungen zu erfüllen, die nach der europäischen Richtlinie 95/46 Anwendung finden, u. a. einschließlich der Standardvertragsbestimmungen für die Übermittlung personenbezogener Daten an Drittländer gemäß der Richtlinie 95/46/EG, und der Anbieter hat diese zu befolgen.

Der Anbieter hat ArcelorMittal alle Prüfberichte zur Verfügung zu stellen, die von der Innenrevision des Anbieters erstellt werden und sich ganz oder teilweise auf die für ArcelorMittal erbrachten Leistungen beziehen.

Darüber hinaus hat der Anbieter den IT Compliance & Security Officer von ArcelorMittal innerhalb von vierundzwanzig (24) Stunden nach einer Sicherheitsverletzung oder mutmaßlichen Sicherheitsverletzung, die den Schutz oder die Sicherheit der Daten von ArcelorMittal (einschließlich personenbezogener Daten) beeinträchtigt hat oder haben kann, schriftlich über diese Sicherheitsverletzung oder mutmaßliche Sicherheitsverletzung zu benachrichtigen. Eine solche Mitteilung muss eine Beschreibung aller vom Anbieter zur Behebung der Verletzung oder mutmaßlichen Verletzung bereits ergriffenen oder noch zu ergreifenden Maßnahmen enthalten.

Der Anbieter hat ArcelorMittal bei der Bearbeitung des Antrags eines Betroffenen auf Zugang zu seinen personenbezogenen Daten umfassend zu unterstützen. Falls der Anbieter von einem Betroffenen direkt aufgefordert wird, Informationen über seine personenbezogenen Daten zu erteilen, hat der Anbieter eine solche Aufforderung sofort an ArcelorMittal weiterzuleiten und der Anbieter darf nicht auf die Aufforderung des Betroffenen reagieren, ohne von ArcelorMittal dazu aufgefordert worden zu sein.

Der Anbieter hat ArcelorMittal auf Aufforderung von ArcelorMittal bei der Erfüllung der Registrierungs- oder sonstigen nach den Datenschutzgesetzen zur Anwendung kommenden Anforderungen, u. a. einschließlich der Bereitstellung angeforderter Informationen und der Registrierung bei den Datenschutzbehörden oder der Beteiligung an selbstregulierenden Programmen zu unterstützen.

Bemerkungen:

In den vorstehenden Vertragsbestimmungen bezeichnet "Anbieter" den Auftragsverarbeiter und "ArcelorMittal" die betreffende Tochtergesellschaft von ArcelorMittal. Falls erforderlich kann der Wortlaut der vorstehenden Bestimmungen an den Wortlaut der Vereinbarung angepasst werden, ohne sich auf den Umfang der Verpflichtungen des externen Auftragsverarbeiters auszuwirken.

Der von der Tochtergesellschaft von ArcelorMittal und dem externen Auftragsverarbeiter geschlossene Vertrag muss auch eine Bestimmung zur "Prüfbefugnis" enthalten. Gemäß dieser Bestimmung ist die Tochtergesellschaft von ArcelorMittal befugt, die Einhaltung der IT-Grundschutzmaßnahmen von ArcelorMittal durch den Anbieter während der Vertragslaufzeit zu prüfen.

(*) Diese *[Bestimmung]* ist nur aufzunehmen, wenn die Wirtschaftseinheit von ArcelorMittal, die diese Vereinbarung schließt, in Europa ansässig ist. Diese Bestimmung gilt nur nach europäischem Recht.

(**) Die im dritten Absatz genannten IT-Sicherheitsrichtlinien sind das Ergebnis der Sicherheitsbewertung. In vielen Fällen handelt es sich dabei um die Sicherheitsrichtlinien des Anbieters, möglicherweise in geänderter Form, um den IT-Grundschutzmaßnahmen von ArcelorMittal zu entsprechen.

Aktuelle Version der Bestimmungen: http://www..... ArcelorMittal Intranet

DEUTSCHLAND

Dies ist eine Sonderversion für Deutschland

Auftragsdatenverarbeitungsvertrag	**Agreement on Data Processing Agency**
1. Anwendungsbereich Im Rahmen der Leistungserbringung nach dem Vertrag vom … [Datum] (nachfolgend „Rahmenvertrag“ genannt) ist es erforderlich, dass der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers oder sonstiger Dritter (nachfolgend „AM-Daten“ genannt) erhält. Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien bei der Durchführung des Rahmenvertrages.	**2. Scope of Application** Rendering the services pursuant to the Framework Contract dating from … including its annexes (hereinafter consistently referred to as “Framework Contract”), it is required that the Agent has access to personal data of the Principal or of other third persons (hereinafter consistently referred to as “AM Data”). This contract shall clearly define privacy data protection law related rights and duties of the parties when executing the Framework Contract.
2. Auftragsdatenverarbeitung 2.1 Der Auftragnehmer erhebt, verarbeitet und/oder nutzt die AM-Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von § 11 BDSG (Auftragsdatenverarbeitung). Der Auftraggeber bleibt im datenschutzrechtlichen Sinn verantwortliche Stelle („Herr der Daten“) und ist für die Rechtmäßigkeit der auftragsgemäßen Erhebung, Verarbeitung und/oder Nutzung der AM--Daten verantwortlich. 2.2 Die Erhebung, Verarbeitung und/oder Nutzung der AM--Daten hat ausschließlich und vollständig innerhalb der Bundesrepublik Deutschland (BRD) und in der/dem in Anlage 1 dieses Vertrages abschließend festgelegten Art, Umfang und Zweck zu erfolgen. Die Erhebung, Verarbeitung und/oder Nutzung der AM--Daten umfasst die in Anlage 1 dieses Vertrages abschließend	**2. Commissioned Data Processing** 2.1 The Agent shall collect, process and/or use the AM Data exclusively in the name and in accordance with the instructions of the Principal in terms of Sec. 11 of the German Federal Data Protection Act (Commissioned Data Processing). The Principal remains the responsible entity in terms of data protection (“data controller”) and is responsible for the legality of collecting, processing and/or using the AM Data as instructed. 2.2 The collection, processing and/or use of AM Data shall exclusively and entirely occur within the Federal Republic of Germany (FRG) and in the type, extent and purpose exclusively defined in Annex 1 to this contract. The collection, processing and/or use of AM Data comprise the type of AM Data and the circle of affected persons exclusively defined in Annex 1 to this contract.

festgelegte Art der AM--Daten und den dort festgelegten Kreis der Betroffenen.	
2.3 Der Auftragnehmer erwirbt an den AM--Daten keine Rechte und ist auf Verlangen des Auftraggebers jederzeit zur Herausgabe der AM--Daten verpflichtet. Zurückbehaltungsrechte in Bezug auf die AM- sind ausgeschlossen.	2.3 The Agent shall not acquire any rights with respect to the AM Data and shall be obliged to return the AM Data at any time on the request of the Principal. Rights of retention in relation to the AM Data are excluded.
2.4 Der Auftragnehmer ist verpflichtet, dem Auftraggeber auf Anfrage zeitnah die für die Erstellung des eigenen Verfahrensverzeichnisses gemäß § 4g Abs. 2 BDSG (Internes Verfahrensverzeichnis des Auftraggebers) erforderlichen Angaben zu machen,.	2.4 The Agent shall, upon request of the Principal and in a timely manner, give full particulars to the Principal to the extent such particulars are required for creating or updating the Principal's internal overview of processing personal data (Sec. 4 lit. g para. 2 of the Federal Data Protection Act).
2.5 Der Auftragnehmer ist verpflichtet, einen betrieblichen Datenschutzbeauftragten schriftlich zu bestellen, soweit er in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt (§ 4f Abs. 1 Satz 1 bis 4 BDSG).	2.5 In case the Agent generally deploys at least ten (10) persons to carry out the automated processing of personal data, the Agent shall be obliged to appoint a data protection official in writing (Sec. 4 lit. f para. 1 s. 1- 4 Federal Data Protection Act).
3. Weisungen des Auftraggebers	**3. Instructions by the Principal**
3.1 Der Auftragnehmer verwendet die vom Auftraggeber übermittelten AM--Daten ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers und der in diesem Vertrag enthaltenen Bestimmungen. Der Auftraggeber behält sich insoweit gegenüber dem Auftragnehmer ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung und -nutzung vor.	3.1 As regards the use of AM Data, the Agent shall be obliged to fully comply with the instructions arising from the Framework Contract and with the instructions issued by the Principal. The Principal reserves the right to instruct the Agent regarding manner, extent and practice of data processing and data usage.
3.2 Die Weisungen des Auftraggebers erfolgen in der Regel schriftlich oder in Textform. In Ausnahmefällen können Weisungen auch mündlich erteilt werden. Mündlich erteilte Weisungen bedürfen jedoch einer unverzüglichen schriftlichen Bestätigung durch den in Ziffer 3.3	3.2 Instructions issued in individual cases shall be issued in writing or by email. In substantiated and individual cases, instructions may as well be issued orally; however, the Principal shall subsequently confirm such instructions in writing or by email and in a timely manner by the

genannten Weisungsberechtigten des Auftraggebers. 3.3 Weisungen dürfen nur von dem Weisungsberechtigten des Auftraggebers oder dessen Stellvertreter erteilt werden. Die Parteien vereinbaren als Weisungsberechtigten des Auftraggebers folgende Person: Weisungsberechtigter: _____ _____ Stellvertreter: _____ _____ 3.4 Ein Wechsel in der Person des Weisungsberechtigten oder seines Stellvertreters oder deren dauerhafte Verhinderung ist der anderen Partei unverzüglich schriftlich unter Benennung eines Vertreters mitzuteilen. 3.5 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Außerdem ist der Auftragnehmer berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen.	authorized person as per Clause 3.3 of this contract. 3.3 Instructions may only be issued by persons authorized to issue instructions and their representatives. The parties agree upon the following persons who will give instructions on behalf of the Principal : Persons Authorized to Issue Instructions: _____ _____ Representative: _____ _____ 3.4 The parties shall inform the respective other party immediately in writing if the responsible persons are changed or hindered. They will name a substitute. 3.5 If the Agent is of the opinion that an instruction violates any statutory regulation and/or a provision of the Framework Contract, the Agent shall be obliged to inform the Principal accordingly and without any undue delay. The Agent shall be entitled to refrain from the execution of such instruction unless the Principal confirms its instruction.
4. Pflichten des Auftraggebers 4.1 Der Auftraggeber ist für die rechtliche Zulässigkeit der Erhebung, Verarbeitung und Nutzung der AM--Daten sowie für die Wahrung der Rechte der Betroffenen verantwortlich. 4.2 Der Auftraggeber ist Eigentümer der AM--Daten und Inhaber aller etwaigen Rechte, die die AM--Daten betreffen.	**4. Obligations of the Principal** 4.1 The Agent acknowledges that the Principal remains responsible for the legality of the processing of AM Data and that the Principal is solely responsible for the protection of the Data subject's rights pursuant to the Data Protection Rules. 4.2 The Principal is the owner of the AM Data and holds all rights in relation to the AM Data.

5. Pflichten des Auftragnehmers	**5. Obligations of the Agent**
5.1 Der Auftragnehmer stellt sicher, dass die Datenverarbeitung und -nutzung im Rahmen der Leistungserbringung nach dem Rahmenvertrag in Übereinstimmung mit den geltenden datenschutzrechtlichen Bestimmungen, insbesondere mit den Bestimmungen des BDSG, mit den Weisungen des Auftraggebers, mit den Bestimmungen des Rahmenvertrages sowie dieses Vertrages erfolgt.	5.1 The Processor undertakes to process and use the AM Data in compliance with the Framework Contract in accordance with applicable Data Protection Rules (especially those of the BDSG) and in compliance with the instructions of the Principal and the provisions of this Agreement.
5.2 Der Auftragnehmer stellt sicher, dass die AM--Daten getrennt von anderen personenbezogenen Daten (insbesondere für andere Auftraggeber verarbeitete personenbezogenen Daten) gespeichert und verarbeitet werden.	5.2 The Agent agrees and warrants that the AM Data will be saved and processed separately from other Data stored on its servers (especially personal data processed for other principals) .
5.3 Der Auftragnehmer darf ohne vorherige schriftliche Zustimmung durch den Auftraggeber keine Kopien oder Duplikate der AM--Daten anfertigen. Hiervon ausgenommen sind lediglich Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen gemäß dem Rahmenvertrag erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.	5.4 The Processor is not allowed to make copies or duplicates of the AM Data without the prior written consent of the Controller, unless such copies or duplicates are necessary or customary to guarantee proper processing of data in accordance with the provisions of the Framework Contract or for the fulfilment of statutory data retention provisions.
5.4 Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden vom Auftragnehmer besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Eingang und Ausgang werden dokumentiert.	5.4 The Agent shall specially mark all media that belong to the Principal or are used on behalf of the Principal. Incoming and outgoing media are subject to constant control that shall be documented.
5.5 Der Auftragnehmer ist verpflichtet, AM--Daten auf Weisung des Auftraggebers unverzüglich zu berichtigen, zu löschen oder zu sperren (§ 35 BDSG).	5.5 The Agent shall be obliged to correct, erase and/or block the AM Data on the Principal's instruction without any undue delay (Sec. 35 of the Federal Data Protection Act).

5.6 Der Auftragnehmer hat dem Auftraggeber auf Anforderung unverzüglich eine Übersicht über die in § 4e S. 1 BDSG genannten Angaben sowie über die zugriffsberechtigten Personen zur Verfügung zu stellen (§ 4g Abs. 2 S. 1 BDSG).	5.6 The Agent shall, upon request of the Principal be obliged to provide the Principal with a summary of the details enumerated in Sec. 4 lit. e cl. 2 of the Federal Data Protection Act and the persons having access to this data (Sect. 4 lit. g para. 2 s. 1 Federal Data Protection Act) without any undue delay.
5.7 Der Auftragnehmer ist verpflichtet, auf Anfrage des Auftraggebers Änderungen der Bestimmungen in Anlage 1 dieses Vertrages zuzustimmen, soweit er keinen sachlichen Grund zur Verweigerung dieser Zustimmung hat.	5.7 On the Principal's request, the Agent shall be obliged to consent to modifications of provisions in Annex 1 to this agreement if and to the extent to which the Agent does not have a factual reason to refuse such consent.
6. Datengeheimnis Der Auftragnehmer hat sämtliche bei der Verarbeitung von AM--Daten beschäftigten Personen gemäß § 5 BDSG schriftlich auf das Datengeheimnis zu verpflichten. Der Auftragnehmer hat weiterhin seine Mitarbeiter zu verpflichten, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und diese Verpflichtung der Mitarbeiter schriftlich zu dokumentieren. Der Auftragnehmer muss dem Auftraggeber auf Anfrage einen geeigneten Nachweis über die Einhaltung dieser Bestimmung liefern.	**6. Data Secrecy** The Agent shall be obliged to commit the persons employed in collecting, processing and/or using AM Data in written form to data secrecy according to Sect. 5 Federal Data Protection Act. The Agent shall also commit its employees to comply with statutory data protection provisions in written form that has to be kept in records. Upon request of the Principal the Agent hast the duty to provide sufficient proof that these obligations are fulfilled.
7. Technische und organisatorische Schutzmaßnahmen 7.1 Der Auftragnehmer garantiert, innerhalb und im Rahmen des ihm nach diesem Vertrag zugewiesenen Verantwortungsbereichs diejenigen technischen und organisatorischen Maßnahmen zu treffen und aufrecht zu erhalten, die erforderlich sind, um die Einhaltung der Bestimmungen dieses Vertrages sowie der anwendbaren	**7. Technical and organizational measures** The Agent guarantees to take the technical and organizational measures - within the Agent's scope and framework of responsibility allotted by the Framework Contract - that are necessary to ensure that the data protection provisions, in particular the provisions of this contract and statutory provisions are

gesetzlichen Datenschutzvorschriften sicherzustellen. Der Auftragnehmer verpflichtet sich vor Verarbeitung der AM--Daten insbesondere – vorbehaltlich weiterer Anweisungen des Auftraggebers – zur Implementierung der in den Baseline Security Controal Measures von AM dieses Vertrages aufgelisteten technischen und organisatorischen Maßnahmen gemäß § 9 BDSG und dem Anhang zu § 9 BDSG. Diese technischen und organisatorischen Maßnahmen können technologischen Weiterentwicklungen angepasst werden. Sämtliche Anpassungen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers.	complied with. In the framework of the automated processing of AM Data, the Agent guarantees subject to further instructions of the principal to particularly take the technical and organizational measures listed in the Baseline Security Control Measures of AM to this agreement ensuring the fulfilment of the requirements of Sec. 9 of the Federal Data Protection Act jointly with the requirements of the appendix to Sec. 9 first sentence of the Federal Data Protection Act. This technical and organizational measures may be adjusted to technological developments. Any adjustments require the written consent of the Principal.
7.2 Im Falle von Abweichungen oder vermuteten Abweichungen von den in vorstehender Ziffer 7.1 enthaltenen Verpflichtungen, wie insbesondere bei jeglichem Verstoß gegen datenschutzrechtliche Bestimmungen, bei Störungen, Problemen oder Fehlern in der Datenverarbeitung, bei Verlust, Entwendung oder unrechtmäßiger Übermittlung von AM--Daten an Dritte sowie bei jeder sonstigen unrechtmäßigen Kenntniserlangung von AM--Daten durch Dritte ist der Auftragnehmer verpflichtet, den IT Compliance & Security Officer des Auftraggebers unverzüglich (d.h. innerhalb von 24 Stunden) über das jeweilige Ereignis (einschließlich der Ursachen, den genauen Zeitpunkt sowie das Ausmaß der Abweichung, die bereits ergriffenen und die noch zu ergreifenden Maßnahmen, etc.) schriftlich zu informieren.	7.2 In cases of any deviation or suspected deviation from the provisions stipulated under clause 7.1, especially any infringement of statutory data protection provisions or failures, problems or malfunctions occurring while processing AM Data or in case of loss, theft or illegal transfer to third parties as well as in case of any other unlawful disclosure to third parties, the Agent shall be, without any undue delay, obliged to inform the IT Compliance & Security Officer of the Principal in writing about the specifics of the respective incident (i.e. in particular about the cause, the precise point in time as well as the extent of the deviation, the already taken and still to be taken measures, etc.) without any undue delay (i.e. within 24 hours).
7.3 Weiterhin ist der Auftragnehmer verpflichtet, bei Geschehnissen im Sinne von Ziffer 7.2 im Benehmen mit dem Auftraggeber unverzüglich sämtliche erforderlichen Maßnahmen einzuleiten, um entstandene Gefährdungen für die Integrität und Vertraulichkeit der AM--Daten zu minimieren und zu beseitigen, die AM--Daten zu sichern und	7.3 In cases of incidents in terms of clause 7.2 of this contract the Agent shall, without undue delay, take any measures necessary for excluding and minimizing any potential risk with respect to the integrity and confidentiality of AM Data, to backup AM Data and to mitigate potential harm of the persons affected. The Agent shall be obliged to co-ordinate with the Principal.
	7.4 Insofar as the Principal has any

Maßnahmen zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. 7.4 Soweit den Auftraggeber Pflichten nach § 42a BDSG treffen, hat der Auftragnehmer ihn hierbei auf erstes Anfordern unentgeltlich im Rahmen des Zumutbaren zu unterstützen.	obligations according to Sect. 42 lit. a Federal Data Protection Act, the Agent shall upon first request by the Principal support the Principal in a reasonable extent free of charge.
8. Kontrollrechte 8.1 Der Auftraggeber ist jederzeit berechtigt, die Geschäftsräume des Auftragnehmers zu betreten sowie zeitlich und räumlich uneingeschränkt die technischen und organisatorischen Maßnahmen sowie die Datenverarbeitungsprozesse im Hause des Auftragnehmers zu prüfen, um sich von der Einhaltung der Bestimmungen dieses Vertrages sowie der einschlägigen gesetzlichen Datenschutzbestimmungen zu überzeugen. 8.2 Der Auftragnehmer gewährt dem Auftraggeber oder einem von diesem beauftragten Dritten in diesem Rahmen die erforderlichen Zugangs-, Auskunfts- und Einsichts-rechte. Der Auftragnehmer verpflichtet sich insbesondere, dem Auftraggeber oder von diesem beauftragten Dritten Zugang zu den Datenverarbeitungseinrichtungen, Dateien und anderen Dokumenten zu gewähren, um die Kontrolle und Überprüfung der relevanten Datenverarbeitungseinrichtungen, Dateien und anderer Dokumentationen zur Verarbeitung und Nutzung der AM--Daten zu ermöglichen. Der Auftragnehmer stellt dem Auftraggeber oder dem von diesem beauftragten Dritten alle für die Kontrolle notwendigen Informationen zur Verfügung. 8.3 Gemäß den Bestimmungen des BDSG unterliegen der Auftraggeber und	**8. Right of Control** 8.1 The Principal shall have the right to accede the business premises of the Agent at any time and unrestricted by time or space in order to inspect the technical and organisational measures and the data processing work flows in the Processor's company and to audit the Agent's compliance with the relevant statutory and contractual data protection provisions. 8.2 The Agent grants to the Principal or any third party assigned by the Principal the necessary rights of access, information and inspection required for the respective audit.Therefore the Agent shall grant to the Principal or third parties assigned by the Principal unimpeded access to all data processing facilities, data files and other documentation to accomplish the inspection and review of all this data processing facilities, data files and other documentation needed for processing AM Data. The Agent provides the Principal or third parties assigned by the Principal with all information necessary for the review. 8.3 The Principal and the Agent may be subject to control by public data protection authorities under the provisions of the Federal Data Protection

der Auftragnehmer öffentlichen Kontrollen durch die zuständige Aufsichtsbehörde. Auf Anforderung durch den Auftraggeber wird der Auftragnehmer die gewünschten Informationen an die Aufsichtsbehörde liefern und dieser die Möglichkeit zur Prüfung im gleichen Umfang einräumen, wie die Aufsichtsbehörde Prüfungen beim Auftraggeber durchführen darf. Davon umfasst sind Inspektionen beim Auftragnehmer durch die Aufsichtsbehörde oder von ihr benannte Personen. Der Auftragnehmer gewährt der zuständigen Aufsichtsbehörde auch in diesem Rahmen die erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte.	Act. Upon request of the Principal the Agent shall provide public data protection authorities with all desired information as well as allow inspections to the same extent the public data protection authorities are authorized to inspect the Principal. This comprises inspections on the Agent's premises by public data protection authorities or persons assigned by those. Therefore the Agent shall grant public data protection authorities the necessary rights of access, information and inspection.
8.4 Im Fall von Kontrollhandlungen und Maßnahmen einer Aufsichtsbehörde beim Auftragnehmer nach § 38 BDSG oder im Fall von Ermittlungen der zuständigen Behörde beim Auftragnehmer nach §§ 43, 44 BDSG hat dieser den Auftraggeber darüber unverzüglich zu informieren.	8.4 In any case of inspections or measures taken by the data protection authorities according to Sec. 38 Federal Data Protection Act or in case of investigations by the competent data protection authorities according to Sec. 43, 44 Federal Data Protection Act on premises of the Agent, the latter shall inform the Principal without undue delay.
9. Beauftragung Dritter 9.1 Der Auftragnehmer ist ohne vorherige schriftliche Zustimmung des Auftraggebers nicht berechtigt, Dritte mit der Verarbeitung oder Nutzung von AM--Daten zu beauftragen. Für mit dem Auftragnehmer im Sinne von §§ 15 ff. AktG verbundene Unternehmen ist eine solche vorherige Zustimmung nicht erforderlich. 9.2 Zur Prüfung einer solchen Zustimmung - bzw. im Falle eines mit dem Auftragnehmer verbundenen Unternehmens zur Information über eine entsprechende Unterbeauftragung - hat der Auftragnehmer dem Auftraggeber eine Kopie der Vereinbarung zur Auftragsdatenverarbeitung zwischen dem Auftragnehmer und dem Dritten zur	**9. Subcontracting to Third Parties** 9.1 The Agent shall not be entitled to subcontracting a third party with the processing or use of AM Data unless the Principal has given its prior written consent to such subcontracting. This does not apply to companies associated with the Agent in terms of Sect. 15 et seqq. German Stock Companies Act. 9.2 For the purpose of assessing such consent and accordingly for the purpose of information regarding subcontracting in case of a company associated to the Agent the latter shall provide the Principal with a copy of the contract regarding the subcontracting the commissioned data processing between the Agent and the third party. By virtue of this contract, the Agent shall bind the third party in writing in such way and to the extent the Agent is obliged towards the Principal

Verfügung zu stellen. In dieser Vereinbarung hat der Auftragnehmer den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftragnehmer aufgrund dieses Vertrages gegenüber dem Auftraggeber verpflichtet ist. Ein Anspruch des Auftragnehmers auf Erteilung der Zustimmung (soweit erforderlich) besteht nicht. 9.3 Der Auftragnehmer hat die Einhaltung der Verpflichtungen des Dritten regelmäßig (d.h. mindestens einmal jährlich) beim Dritten zu überprüfen und den entsprechenden Prüfbericht dem Auftraggeber nach Abschluss der Prüfung unverzüglich zur Verfügung zu stellen.	pursuant to contract. However, the Principal shall not be under any obligation (if consent is necessary) to declare such a consent. 9.4 The Agent shall regularly (i.e. at least once a year) control whether a subcontracted third party complies with its obligations arising from the contract concluded between the Agent and the third party, and shall provide the Principal with the relevant written inspection report without undue delay after the respective inspection of the subcontractor.
10. Rechte der Betroffenen 10.1 Die Rechte der durch die Datenverarbeitung betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen. 10.2 Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung, Löschung oder Sperrung der ihn betreffenden Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. 10.3 Für den Fall, dass eine betroffene Person ihre Rechte auf Berichtigung, Löschung oder Sperrung von AM--Daten sowie auf Auskunft über die gespeicherten AM--Daten, den Zweck der Speicherung und die Personen und Orte, an die AM--Daten regelmäßig übermittelt werden, geltend macht, ist der Auftragnehmer verpflichtet, den Auftraggeber bei der Erfüllung dieser Anforderungen zu unterstützen.	**10. Rights of data subjects (persons affected)** 10.1 Data subjects affected by the data processing may exercise their rights vis-à-vis the Principal only. 10.2 As far as data subjects contact the Agent to exercise their rights to information, correction, erasure or blocking of the personal data affecting them, the Agent shall forward those requests to the Principal without undue delay. 10.3 In case that a data subject exercises its rights to information, correction, erasure or blocking of AM Data as well as disclosure of stored AM Data, the purpose of storage and the persons and places to which AM data are transferred regularly the Agent is obliged to support the Principal to fulfil those obligations.
11. Auskunft an Dritte	**11. Information of Third Persons**

11.1 Soweit der Auftragnehmer aufgrund gesetzlicher Bestimmungen Dritten Auskunft über AM--Daten erteilen muss, ist der Auftragnehmer verpflichtet, den Auftraggeber vor Auskunftserteilung über den Empfänger, Zeitpunkt und Inhalt der zu erteilenden Auskunft schriftlich zu informieren. 11.2 Im Übrigen darf der Auftragnehmer Auskünfte über AM--Daten an Dritte oder Betroffene nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.	11.1 If and to the extent the Agent is obliged to provide information concerning AM Data to a third party due to a mandatory statutory provision, the Agent is, prior to the provision of such information, obliged to inform the Principal in writing about the identity of the third party, the point in time and the specific information to be given. 11.2 Apart from that case the Agent may provide information about AM Data to third parties only with the prior written consent of the Principal.
12. Löschung von Daten und Rückgabe von Datenträgern 12.1 Der Auftragnehmer hat ihm überlassene und alle ergänzend hinzugewonnenen AM--Daten, Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, vollständig und unwiderruflich zu löschen oder zu vernichten sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, spätestens jedoch nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung des Rahmenvertrages). Gleiches gilt für Vervielfältigungen der AM--Daten (insbesondere Archivierungs- und Sicherungsdateien) in allen Systemen des Auftragnehmers sowie Test- und Ausschussdaten, Notizen, Mitschriften, Entwürfe und Kopien. 12.2 Das Protokoll über die Löschung bzw. Vernichtung der AM- Daten ist dem Auftraggeber auf Anforderung unverzüglich vorzulegen. 12.3 Dokumentationen, die dem Nachweis der auftrags- und	**12. Return and Deletion of Data** 12.1 The Agent shall completely and irrevocably erase or destroy all AM Data handed over to the Principal as well as any additionally collected AM Data, data resulting from processing and use as well as data associated to the contract as soon as the knowledge of those data is no longer required for the fulfilment of the purpose of storage, however, at the latest subsequently to the fulfilment of rendering the service(s) covered by the Framework Contract (in particular subsequently to the cancellation or to any other termination of the Framework Contract). This clause also applies for duplication of AM Data (including backups for archiving and security reasons) on any of the Agent's systems as well as test data, junked data, notices, notes, drafts and copies. 12.2 Upon request of the Principal, the Agent shall be obliged to make available to the Principal the protocol over the erasure or deletion of the AM Data without undue delay. 12.3 Documentation required to prove data processing according to contractual

ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.	and legal provisions shall be retained by the agent after the rendering of this contract for the duration of the particular retention period.
13. Schlussbestimmungen Die Dauer der Datenverarbeitung im Auftrag richtet sich nach den Bestimmungen zur Laufzeit des Rahmenvertrags. Änderungen, Ergänzungen und eine Aufhebung dieses Vertrages bedürfen der Schriftform. Gleiches gilt für eine Änderung des Schriftformerfordernisses. Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der betreffenden unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem wirtschaftlichen Zweck der unwirksamen Regelung am nächsten kommt bzw. diese Lücke ausfüllt.	**13. Final provisions** The duration of the Commissioned Data Processing shall be dependent on the provisions concerning the duration of the Framework Contract. Alterations, amendments and the termination of this contract shall be made in writing. This also applies for an amendment of this provision. Should a provision of this contract be or become invalid as well as be incomplete, the validity of the other provisions of this Agreement shall remain unaffected hereby. The parties agree that, in the place of the invalid provision, a legally binding provision shall apply which comes closest to what the parties would have agreed if they had taken the partial invalidity or incompleteness into consideration.

_____ _____

Ort, Datum / Place, Date Ort, Datum / Place, Date

_____ _____

Unterschrift (Auftraggeber) Unterschrift
(Auftragnehmer)

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kreis der Betroffenen / Appendix 1: Purpose, type and extent of data processing, type of data and affected persons

1. Zweck der Datenverarbeitung / Purpose of Data Processing,
2. Art und Umfang der Datenverarbeitung / Type and Extent of Data Processing
3. Art der Daten / Type of Data
4. Kreis der Betroffenen / Affected Individuals

ANHANG VI

PS: Aus Sicherheitsgründen wird dieser ANHANG VI in der außerhalb von ArcelorMittal veröffentlichten Version freigelassen. Dieser ANHANG VI wird in die Ausfertigung des im Intranet veröffentlichten Verfahrens aufgenommen.

Datenschutzkorrespondenten

Aktuelle Version dieser Liste: http://www.....arcelormittal Intranet

ITCS Officers

Aktuelle Version dieser Liste: http://www.....arcelormittal Intranet

ANHANG VII

Prüffragebogen

Prüfung der Einhaltung der Datenschutzbestimmungen

Checkliste

Name der Softwareanwendung/Datenbank

Zweck der Anwendung

Name/Abteilung des für diese Anwendung Verantwortlichen
. IT-Aspekte
. Funktionsaspekte

Wer sind die Betroffenen?
(alle Mitarbeiter von ArcelorMittal? Oder eine spezifische Kategorie von Mitarbeitern von ArcelorMittal? Kunden von ArcelorMittal? …)

Wie viele Betroffene gibt es in diesem Prozess?
(ungefähre Angabe)

Welche personenbezogenen Daten gibt es in diesem Prozess?
(Bildschirmabbildungen)

Liegen sensible Daten vor?

Woher stammen die Daten?
(Mit anderen Worten, welches sind die Datenquellen?) Direkt vom Betroffenen? Oder woher?

Wie lange werden die Daten gespeichert?

Wer hat Zugang zu den Daten?
. innerhalb von ArcelorMittal
. außerhalb von ArcelorMittal

Zugang zu den Daten: Von wo? Gibt es eine grenzüberschreitende Datenübermittlung?

Erfolgt eine Migration der Daten zur Verwendung in anderen Anwendungen?
Falls ja: welche Anwendung?

Recht des Betroffenen, auf seine Daten zuzugreifen: wie informieren Sie den Betroffenen über seine Zugriffsrechte?

Ist ein Dritter (innerhalb oder außerhalb von ArcelorMittal) an dem Prozess beteiligt?

Falls ja: zu welchem Zweck (z. B. Hosting…)?

Wurden (ggf.) Informationen über die Anwendung weitergegeben?

Welche Sicherheitsmaßnahmen sind vorhanden?

Aktuelle Version dieses Fragebogens: http://www.....arcelormittal Intranet

ANHANG VIII

Beschreibung der Datenverarbeitung

Kategorien von Daten

Personaldaten

Kommerzielle Daten

IT-Daten

Daten zur sozialen Verantwortung der Gesellschaft

Arbeitsschutzdaten

Betroffene

Die meisten Betroffenen, deren Daten verarbeitet werden, sind Mitarbeiter von ArcelorMittal.

Neben den Mitarbeitern von ArcelorMittal sind die Betroffenen, deren Daten von ArcelorMittal verarbeitet werden:
. Kundenvertreter (ArcelorMittal unternimmt "B2B"-Aktivitäten ohne Kunden in seinem Kundenportfolio)
. Anbietervertreter
. Auftragnehmer, die im Namen von ArcelorMittal tätig sind
. Lokale Interessensgruppen

Personaldaten

Zweck der Übermittlung/Verarbeitung

Personalverwaltung und -management, einschließlich Mitarbeitersuche, Gehaltszahlung, Karriereplanung und Koordinierung von Fähigkeiten, Schulungen (E-Learning), Verwaltung der Leistungen an Mitarbeiter, Leistungsbewertung der Mitarbeiter, Pflege der Mitarbeiterdatenbanken, Einhaltung der zur Anwendung kommenden gesetzlichen Anforderungen.

Kommerzielle Daten (Personenbezogene Daten in Bezug auf Kunden, Lieferanten und Geschäftspartner jeglicher Art).
Die Personen werden als Ansprechpartner von ArcelorMittal innerhalb eines Unternehmens geführt, die das Unternehmen repräsentieren.

Zweck der Übermittlung/Verarbeitung

Ausführung und Verwaltung von Geschäftsprozessen, einschließlich Gehaltsaktivitäten, Einkaufsaktivitäten, Buchhaltung und Controlling, Verwaltung der Vermögenswerte der Unternehmen, Einhaltung der zur Anwendung kommenden gesetzlichen Anforderungen.

IT-Infrastrukturmanagement, einschließlich E-Mail, Zugang zum ArcelorMittal Intranet, Einsatz von gemeinsam nutzbaren Tools und ganz allgemein Verwaltung des Benutzerzugangs zu IT-Anwendungen;

Daten zur sozialen Verantwortung der Gesellschaft

Zweck der Übermittlung/Verarbeitung

Soziale Verantwortung der Gesellschaft, einschließlich des Verständnisses für unser betriebliches Umfeld und die Bedenken von Interessensgruppen, Verwaltung des laufenden Programms von ArcelorMittal für das Engagement in den Gemeinschaften vor Ort.

Arbeitsschutzdaten

Zweck der Übermittlung/Verarbeitung

: Arbeitsschutzprozesse umfassen Aktivitäten zur Sicherstellung der Sicherheit und des Schutzes der Arbeitnehmer und Ressourcen von ArcelorMittal. Beispiele sind u. a. der Arbeitsschutz und die Authentifizierung des Mitarbeiterstatus für den Zugang zu den Ressourcen und Einrichtungen von ArcelorMittal.

ANHANG IX

PS: Aus Sicherheitsgründen wird dieser ANHANG VI in der außerhalb von ArcelorMittal veröffentlichten Version freigelassen. Dieser ANHANG VI wird in die Ausfertigung des im Intranet veröffentlichten Verfahrens aufgenommen.

Data Protection Committee

Die vom Group CIO ernannten anfänglichen Mitglieder des Data Protection Committee sind
. [Name 2]
Die vom EVP Human Resource ernannten anfänglichen Mitglieder des Data Protection Committee sind
. [Name 2]
Der anfängliche Schriftführer ist: Emmanuel CAUVIN